AWS Well-Architected Framework

Supply Chain Lens

Supply Chain Lens: AWS Well-Architected Framework

Table of Contents

Supply Chain Lens - AWS Well-Architected Framework

Publication date: **September 9, 2025** (*Document revisions*)

The Well-Architected Supply Chain Lens describes the customer user scenarios and pillar questions, best practices, and Implementation guidance for customers building and managing their supply chain workloads on AWS.

Introduction

The AWS Well-Architected Supply Chain Lens is a collection of customer-proven best practices for designing Well-Architected supply chain workloads. The Supply Chain Lens contains insights, key design elements and recommendations that AWS has gathered from real-world case studies. The Supply Chain Lens is built upon six fundamental pillars: operational excellence, security, reliability, performance efficiency, cost optimization and sustainability. This framework provides a consistent approach for customers and partners to evaluate architectures, remediate risks, and implement designs that deliver business value.

Supply chain covers a wide range of services such as manufacturing, inventory planning, warehouse and distribution, labor planning, materials and facilities management in addition to variety of transportation and logistics services like airfreight, maritime, trucking, and rail. It is an assets-intensive horizontal across multiple industries. Therefore, supply chain companies own a large stack of technologies designed and configured based on the catalogue of services they offer their customers. Typically, there is a mix of third-party technologies configured and customized, along with in-house developments to cover their business needs.

The Supply Chain Lens provides implementation guidance for different scenarios in a supply chain customer cloud journey. It helps customers manage their workloads of different software vendors ISVs such as ERPs and TMS solutions in an efficient and cost-efficient approach. The lens also recommends the AWS services that best supports the development and integration of new solutions in a secure and reliable architecture. The Supply Chain Lens helps you consistently measure your architectures against best practices and identify areas for improvement.

This document is intended for those in technology roles, such as chief technology officers (CTOs), chief information security officers (CISOs), architects, developers, compliance officers, and operations team members. After reading this document, you will understand AWS best practices and strategies to use when designing architectures for the development and deployment of supply chain workloads and applications.

Custom lens availability

Custom lenses extend the best practice guidance provided by AWS Well-Architected Tool. AWS WA Tool allows you to create your own custom lenses, or to use lenses created by others that have been shared with you.

To determine if a custom lens is available for the lens described in this whitepaper, reach out to your Technical Account Manager (TAM), Solutions Architect (SA), or Support.

Definitions

The AWS Well-Architected Framework is based on six pillars: operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability. AWS provides multiple core components that allow you to design state-of-the-art architectures for your Supply Chain workloads. In this section, we will present an overview of key definitions that will be used in this document.

Today's supply chain customers vision is to augment existing systems (repeal and replace where needed), processes, and people by building a resilient supply chain layer with single pane of glass (SPOG) to view across the organization. This organization uses data-driven, responsive decision-making infrastructure with integrated data system as a foundational building block aided by purpose-built services like artificial intelligence (AI) and machine learning (ML). Such systems can help improve visibility, agility, efficiency, and risk management of an organization while reducing time-to-value realization and expediting the time to market.

Organizations have multiple work streams within their supply chain business which operate interdependently, with integrated upstream and downstream systems enabling efficient information exchange. This integration is required to exchange information with as little latency as possible. The work streams include demand and supply, planning and forecasting, supplier management, inbound and outbound logistics, material flow and tracking, and sustainability.

Supply chain: A supply chain is the network of individuals, organizations, resources, activities and technologies involved in the creation and scaling of a product. Supply chains manage the flow of materials and products from suppliers through manufacturers to end consumers, including all distribution processes.

Supply chain management (SCM): Supply chain management is a broad term that covers the planning and management of all activities involved in sourcing, procurement, conversion, and logistics of goods or services. It also involves the coordination and collaboration with channel partners such as suppliers, 3rd party service providers and customers and it aims to integrate supply and demand management within and across the organization.

Logistics management: Logistics management is a subset of SCM that focuses on efficient and effective flow and storage of materials, services and related information from the point of origin to the point of consumption. Logistics management activities are normally separated as Inbound and Outbound logistics which includes transportation, warehousing, inventory, order fulfillment, and network design.

Capacity management: Capacity management calculates supplier volume capacity and component consolidation, aggregating data at various levels (part numbers, part groups) for both short-term and long-term fulfillment planning. This process predicts product shortages and enables manufacturers to plan sourcing proactively.

Supplier management: Supplier management is the process of identifying, qualifying, onboarding, transacting and collaborating with the suppliers of materials/goods that are essential for a business or building a product. It involves managing the relationships, performance, risk, and contracts of the supplier. Supplier management helps a business to optimize its supply chain, reduce costs, improve quality and enhance innovation. The supplier can be at different levels known as tiers. For example, Tier 1, Tier 2, to Tier N suppliers.

Warehouse management system (WMS): Warehouse management system is a software solution that offers visibility into a business inventory and manage fulfillment operations. The inventory management is usually aligned to production schedules and its synchronized, orchestrated material feed to make sure parts required at each workstation on assembly line are available, without manual intervention. The activities generally involve:

- Material planning by connecting with supply planning
- Material flow orchestration by connecting inbounds, pick-ups, material feeds at line or station levels
- Process confirmation based on in-station feedback to the assembly workers.
- Action recognition and confirmation based on In-station corrective feedback in connection with the manufacturing shop-floor.

Transport or fleet management: Transport management is the process of planning, implementing, and controlling the efficient and effective movement and storage of goods or services from the point of origin to the point of consumption. It is a key component of supply chain management as it affects the cost, quality and customer satisfaction of the delivered goods. Activities involved in the transport management are:

- Transport mode selection (air, road, or sea) based on speed, cost and environmental impact.
- Route optimization selection based on distance, traffic, weather, road condition.
- Carrier selection based on the best carrier with high efficiency rate.
- Performance analysis based on performance of the transport operations, using on-time delivery, fuel-consumption, and carbon footprints.

- Track and trace of transports in real-time based on the geo-fencing to make sure the on-time delivery and contingency planning.

Sustainability management: Sustainability management is the practice of integrating environmental and social values into the supply chain operations, from sourcing to delivery. It aims to minimize the negative impact and maximize the positive impact of the supply chain activities on the planet. The sustainability measurements in the supply chain management are categorized into

- Environmental sustainability involves reducing the greenhouse gas emissions, energy consumption, water usage, waste generation, and pollution caused by the supply chain processes

Social sustainability involves facilitating the fair and ethical treatment of the workers, suppliers, customers, and communities involved in the supply chain. It also involves respecting the human rights, labor standards, health and safety, and diversity and inclusion of the stakeholders.

Design principles

The Well-Architected Framework identifies a set of general design principles to facilitate good design in the cloud. The following design principles should be considered when designing and operating supply chain workloads:

- **Design for global distribution and regulatory compliance:** Supply chain operations frequently span multiple Regions and jurisdictions, each with distinct regulatory requirements. Design applications that can operate across diverse geographical locations while maintaining compliance with local laws, data residency requirements, and industry-specific regulations. Implement automated compliance monitoring, Region-specific configurations, and data governance controls that adapt to local requirements. Consider regulatory variations in data protection, trade compliance, customs requirements, and industry standards when architecting your global supply chain systems. Design for high availability across multiple geographical locations to maintain business continuity and resilience against regional disruptions.
- **Prioritize security across the extended supply chain environment:** Supply chain environments involve complex data sharing relationships with suppliers, customers, partners, and regulatory bodies. Implement a Security by Design approach that addresses the unique challenges of multi-party data exchange. Encrypt all sensitive data including supplier information, customer data, pricing details, and intellectual property both at rest and in transit. Establish robust identity and access management for partner integrations, implement API security controls, and maintain comprehensive audit trails for all supply chain transactions. Design security controls that can accommodate the dynamic nature of supply chain partnerships while maintaining strict data protection standards.
- **Build integration-first architectures for environment connectivity**: Supply chain success depends on seamless integration across suppliers, customers, logistics providers, and regulatory systems. Design integration patterns that prioritize API-first architectures, event-driven messaging for real-time supply chain events, and standardized data formats to reduce transformation complexity. Implement scalable partner onboarding frameworks that can accommodate growth in your supplier network without operational overhead. Make sure integration strategies support both traditional protocols (such as EDI) and modern APIs to accommodate diverse partner technical capabilities and existing ERP, TMS, and warehouse management systems. Design for reliable data exchange that can handle intermittent connectivity and varying partner system availability across your global supply chain network.
- **Scale dynamically to accommodate demand volatility:** Supply chain operations experience significant fluctuations driven by seasonality, market changes, and unexpected events. Design

systems that can scale elastically to handle peak periods while optimizing costs during lower demand phases. Use On-Demand Capacity Reservations (ODCR) for predictable seasonal peaks and dynamic scaling for unexpected demand spikes. Implement comprehensive load testing to validate system performance under various demand scenarios. Design caching strategies, content delivery networks, and database architectures that can handle varying transaction volumes while maintaining consistent performance for critical supply chain processes.

- **Design for supply chain resilience and business continuity:** Supply chains face unique disruption risks including natural disasters, geopolitical events, supplier failures, transportation interruptions, and demand shocks that can cascade across manufacturing, warehousing, and distribution operations. Design architectures that can rapidly adapt to supply chain disruptions through automated failover to alternate suppliers, dynamic inventory rebalancing, and flexible logistics routing. Implement risk monitoring systems that can identify potential disruptions early and trigger automated response procedures across your supply chain network. Design supply chain networks with built-in redundancy and the ability to quickly reconfigure operations when primary suppliers or transportation routes become unavailable. Plan for scenarios where entire regions or supplier networks may become temporarily inaccessible, considering the asset-intensive nature of supply chain operations.
- **Establish comprehensive data governance for supply chain master data**: Supply chain operations depend on accurate, consistent master data including product catalogs, supplier information, customer records, and inventory data that must be synchronized across multiple systems and trading partners. This is particularly critical given the mix of third-party technologies and in-house developments typical in supply chain environments. Implement data governance frameworks that maintain data quality, consistency, and lineage across your supply chain environment spanning manufacturing, inventory planning, warehouse operations, and transportation management. Design master data management processes that can handle the complexity of multi-party data relationships while maintaining single sources of truth for critical supply chain entities. Establish data quality monitoring and automated correction processes to help prevent data inconsistencies from propagating through your ERP, TMS, and other supply chain systems and causing operational disruptions.
- **Implement comprehensive observability for supply chain visibility:** Establish end-to-end observability that spans your entire supply chain technology environment, from infrastructure performance to business process execution. Implement comprehensive logging for all system activities and data access, with particular attention to supply chain events such as shipment updates, inventory changes, and order fulfillment. Maintain log immutability for audit and compliance purposes, which is critical for supply chain traceability requirements. Configure proactive monitoring and alerting for key supply chain metrics including inventory levels,

supplier performance, shipment delays, and order fulfillment rates. Create dashboards that provide real-time visibility into supply chain KPIs and enable rapid response to disruptions or performance issues.

Scenarios

The AWS Well-Architected Framework provides architectural guidance for building effective supply chain solutions. This section presents eight scenarios demonstrating how AWS services solve specific supply chain challenges, from planning and forecasting to warehouse automation and product traceability. Each scenario includes a description of typical use cases and reference architecture with metrics aligned to Well-Architected principles.

These scenarios showcase practical applications of AWS technologies including artificial intelligence, machine learning, and analytics capabilities. Organizations can use these architectures as blueprints to improve their supply chain visibility, automate operations, optimize inventory, and enhance decision-making. The solutions incorporate security, reliability, performance efficiency, and cost optimization best practices while maintaining operational excellence through AWS services.

Planning and operations

Supply chain planning and operations involve managing the flow of goods, services, and information from suppliers to end customers. This complex process encompasses demand forecasting, inventory management, procurement, production scheduling, warehousing, transportation, and distribution activities. Organizations use supply chain planning to optimize their resources, reduce costs, minimize risks, and make timely delivery of products to customers. Effective supply chain operations require careful coordination among various stakeholders, including suppliers, manufacturers, distributors, retailers, and logistics providers.

AWS offers a powerful combination of Amazon SageMaker AI's machine learning capabilities and Amazon Bedrock's generative AI models to revolutionize supply chain planning and operations. In demand planning and forecasting, while SageMaker AI processes historical sales data and market trends to create statistical forecasting models, Bedrock's Claude or Titan models analyze unstructured data sources like news articles, social media trends, and market reports to identify emerging patterns that might impact demand. This combined approach provides more comprehensive and nuanced demand predictions than traditional forecasting methods alone.

In manufacturing operations, Amazon SageMaker AI builds predictive maintenance models that analyze equipment sensor data to forecast potential failures days or weeks in advance, reducing unplanned downtime. Amazon Bedrock enhances these insights by generating equipment-specific

maintenance procedures, step-by-step troubleshooting guides, and repair documentation tailored to detected anomalies.

Anthropic's Claude analyzes historical maintenance logs alongside technical documentation to identify recurring issues and suggest optimization opportunities, such as modified maintenance intervals or alternative replacement parts, resulting in a more proactive maintenance program that extends equipment lifespan.

For capacity planning, SageMaker AI algorithms optimize production schedules by analyzing historical throughput data, labor constraints, and material availability, while Bedrock generates detailed production scenarios for various demand patterns, equipment configurations, and workforce levels.

This enables manufacturing planners to evaluate multiple operational strategies through intuitive natural language interfaces where they can conversationally query complex scheduling scenarios, such as *What happens to our production capacity if supplier X delays deliveries by two weeks?*

In logistics and distribution, SageMaker AI powers route optimization models that reduce transportation costs and inventory management systems that decrease holding costs while maintaining service levels.

Bedrock complements these capabilities by generating comprehensive logistics execution plans containing carrier-specific handling instructions, temperature control requirements, customs documentation checklists, and contingency procedures for disruptions like port congestion or weather events.

Claude analyzes complex shipping documentation against constantly changing customs regulations for different countries, identifying compliance issues before shipment and suggesting corrective actions that significantly reduce the risk of costly delays and regulatory penalties.

For supply chain risk management, SageMaker AI analyzes quantifiable risk factors such as historical supplier performance, lead time variability, and demand volatility, while Bedrock continuously monitors news feeds, weather forecasts, labor disputes, and geopolitical developments affecting key trade routes or production regions.

This combined approach enables the generation of comprehensive risk reports with financial impact assessments, probability ratings, and prioritized mitigation recommendations tailored to specific business constraints.

Supplier relationship management benefits significantly from SageMaker AI's ability to evaluate comprehensive supplier performance metrics including quality, on-time delivery, responsiveness,

and cost competitiveness, creating segmentation models that identify which suppliers require closer partnership versus transactional relationships.

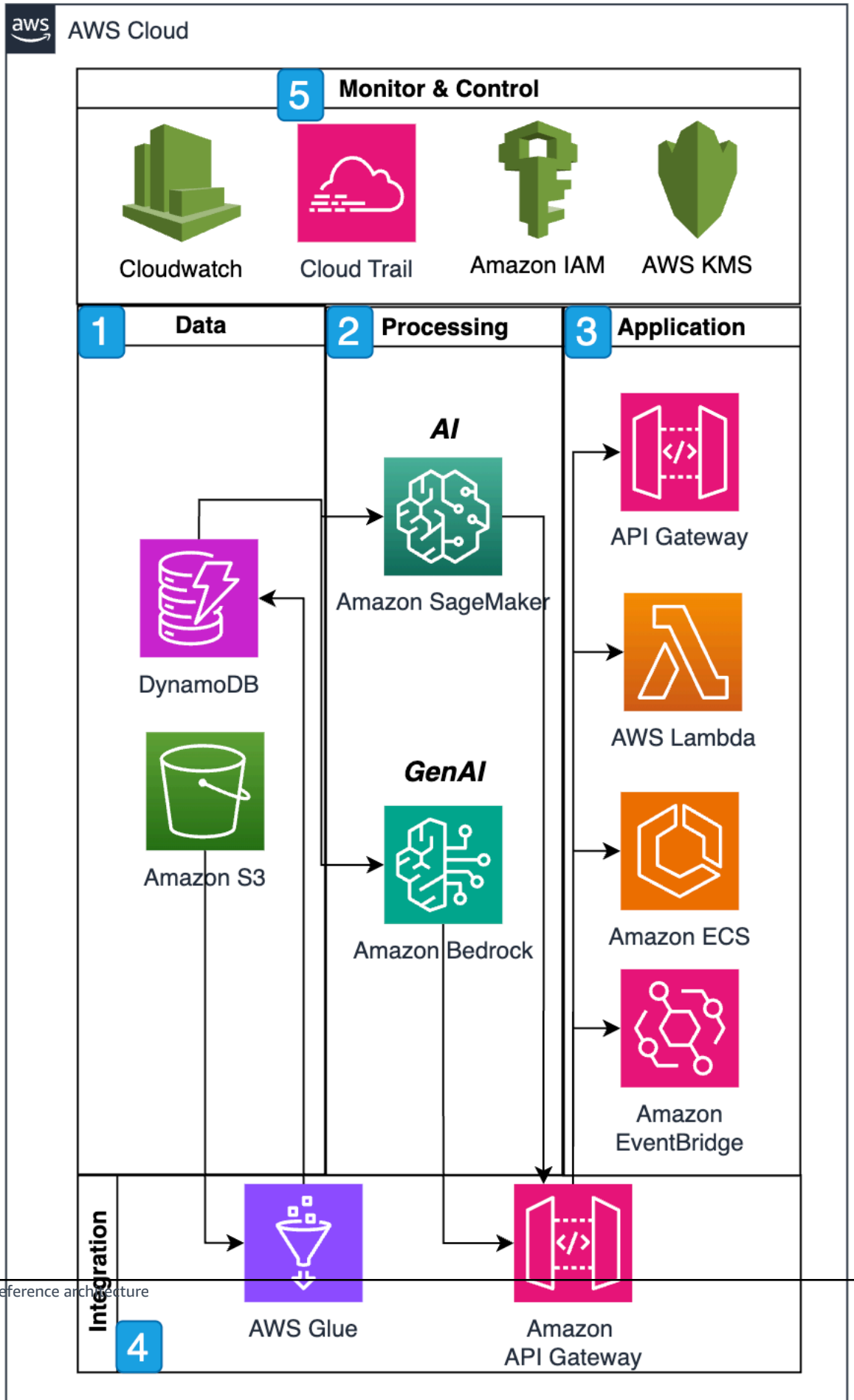
Bedrock assists procurement teams by generating professional correspondence such as RFP documents, contract amendment requests, and negotiation position summaries based on specific business requirements and supplier history.

Claude analyzes complex supplier proposals and contract language to identify favorable terms, potential risks, hidden costs, and negotiation opportunities, improving overall supplier governance and relationship management.

Implementation of these supply chain solutions follows a structured approach in Amazon SageMaker AI Studio: setting up the environment with appropriate IAM permissions; integrating supply chain data from ERP systems, IoT devices, and external sources; developing and training appropriate models for specific use cases; connecting to Bedrock services for natural language capabilities; creating automated pipelines for ongoing operations; deploying models as scalable endpoints; and integrating these intelligent capabilities into existing supply chain workflows and systems through well-documented APIs and user interfaces.

The integration of SageMaker AI's machine learning capabilities with Bedrock's generative AI creates a more comprehensive supply chain management solution. This combination enables organizations to handle both quantitative analysis and qualitative insights, while providing natural language interfaces that make complex supply chain operations more accessible to users across the organization. The system can continuously learn and adapt to new conditions while generating actionable insights and recommendations in human-readable formats. This integrated approach helps organizations maintain optimal inventory levels, respond quickly to market changes, verify product quality, and ultimately enhance customer satisfaction while maximizing operational efficiency and profitability.

Reference architecture



Architecture description

1. Data ingestion from various sources.
2. Processing through ML models and AI services.
3. Real-time analysis and prediction.
4. API-based service delivery.
5. Continuous monitoring and optimization.

Architecture objectives

- Scalable processing of supply chain data.
- Real-time insights and predictions.
- Secure and compliance-aligned operations.
- Integration with existing systems.
- Monitoring and optimization capabilities.

Metrics

Based on the supply chain planning and operations scenario, the three recommended metrics for an AWS Well-Architected Framework analysis, along with their rationale are:

1. Simulation accuracy:
    - **Metric**: Percentage accuracy of simulations predicting the impact of changes in transportation strategies.
    - **Rationale**: This directly measures the reliability and effectiveness of the combined SageMaker AI and Bedrock solution in making accurate predictions, which is fundamental to the entire system's value proposition.
    - **Target**: Over or equal to 90% accuracy in predictions when compared to actual outcomes.
    - **Well-Architected pillars**: Performance efficiency and reliability.
2. Route optimization savings:
    - **Metric**: Dollar savings achieved through last-mile and middle-mile route optimizations.
    - **Rationale**: Provides concrete financial validation of the system's effectiveness and demonstrates clear business value.

- **Target**: Minimum 15% reduction in transportation costs.
- **Well-Architected pillars**: Cost optimization and performance efficiency.

3. Frequency of emergency responses:
   - **Metric**: Number of emergency responses or corrective actions triggered by the application. For Example:
     - Supply chain disruptions like weather, political, labor or other developments impacting logistics or trade routes.
     - Equipment Failures flagged as imminent requiring immediate intervention.
     - Compliance issues impacting customs processing time or penalties.
     - Inventory shortages impending based on plan including supplier performance issues or unexpected demand spikes.
     - Quality control failures requiring immediate corrective action.
   - **Rationale**: Indicates the system's effectiveness in proactive risk management and its ability to prevent disruptions.
   - **Target**: Over or equal to 30% reduction in emergency incidents year-over-year.
   - **Well-Architected pillars**: Reliability and operational excellence.

These metrics were selected because they:

- Directly align with core AWS Well-Architected Framework pillars.
- Provide measurable evidence of system effectiveness.
- Cover both technical performance and business outcomes.
- Address key aspects of the scenario: prediction accuracy, cost optimization, and risk management.

Procurement automation

Implementing machine learning (ML) based procurement automation in the supply chain using AWS services and the AWS Well-Architected Framework provides organizations with a robust and scalable solution. AWS offers a comprehensive suite of services that transform traditional procurement processes into intelligent, automated workflows.

The procurement automation system uses multiple AWS services to create an intelligent end-to-end solution. Amazon Textract analyzes supplier documentation using Optical Character

Recognition (OCR) to extract key information from unstructured text. AWS Bedrock's Claude model processes this extracted document information to analyze and categorize complex procurement documents, including RFQs, purchase orders, and contracts, while maintaining compliance with organizational policies and regulatory requirements.

The solution automates key procurement workflows through intelligent integration of AWS services. AWS Lambda functions trigger automated actions based on predefined conditions, such as generating purchase orders when specific criteria are met or initiating supplier reviews based on performance metrics. Amazon EventBridge orchestrates these workflows, for smooth coordination between different procurement processes and systems.

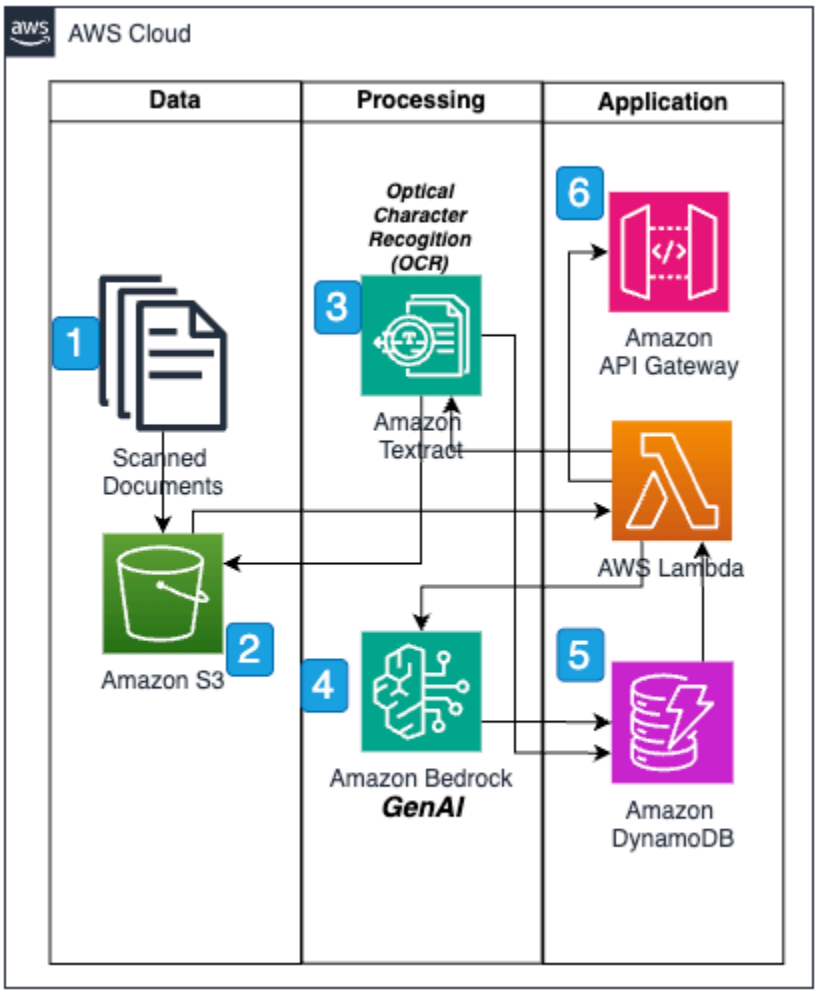
AWS Bedrock's generative AI capabilities enhance the procurement process through intelligent document generation and analysis. The system can automatically create detailed supplier communications, analyze responses, and generate comparison reports. Claude can evaluate complex contract terms, identify potential risks, and suggest optimizations based on historical procurement patterns and market conditions.

For supplier relationship management, the solution combines SageMaker AI's analytical capabilities with Bedrock's natural language processing to provide comprehensive supplier insights. Amazon SageMaker AI provides sophisticated model training and optimization capabilities, allowing companies to develop custom models for supplier evaluation, risk assessment, and price optimization using their historical procurement data. The system monitors supplier performance, generates automated performance reviews, and creates improvement plans when needed. Amazon Comprehend analyzes supplier communications and feedback to identify potential issues or opportunities for relationship enhancement.

Security and compliance are paramount in procurement operations. The AWS Well-Architected Framework makes sure that the solution implements robust security controls, including encryption of sensitive procurement data, fine-grained access controls, and comprehensive audit trails. AWS CloudTrail and Amazon GuardDuty provide continuous security monitoring and threat detection to protect procurement operations.

Together, these AWS services create a sophisticated procurement automation solution that reduces manual effort, improves decision-making, and enhances supplier relationships. Organizations can handle both structured and unstructured procurement data while providing intuitive interfaces for procurement teams. The system continuously learns from procurement patterns and outcomes, helping organizations optimize their purchasing strategies, reduce costs, and maintain healthy supplier relationships while supporting compliance with organizational policies and regulatory requirements.

Reference architecture



Architecture description

1. Scanned documents are saved into Amazon S3.
2. AWS Lambda processes these documents through Amazon Textract.
3. Extracted data from the scanned documents are saved into Amazon S3.
4. AWS Lambda processes these documents through Amazon Bedrock for analysis, categorization, and generating additional information like summaries.
5. AWS Lambda posts the output to Amazon DynamoDB.
6. API integration is used to post the processed results

Architecture objectives

- Process automation
- Intelligent document processing
- Supplier management
- Cost optimization
- Continuous improvement
- Integration and scalability

Metrics

Three recommended metrics for the procurement automation scenario are:

- Supplier performance score:
  - **What**: Measures overall supplier effectiveness and reliability
  - **Why**: Directly tracks the AI/ML system's ability to evaluate and manage suppliers
  - **Target**: 95% or higher performance rating
  - **Calculation**: Weighted average of:
    - Delivery accuracy (30%)
    - Quality compliance (30%)
    - Response time (20%)
    - Policy compliance (20%)

- SLA compliance rate:
  - **What**: Measures system's ability to meet service level agreements
  - **Why**: Critical for validating automation effectiveness
  - **Target**: 98% or higher compliance
  - **Key components:**
    - Document processing time
    - Order accuracy
    - System availability
    - Response times

- Perfect order rate:
  - **What**: Measures end-to-end procurement success
  - **Why**: Validates overall system effectiveness
  - **Target**: 99% or higher perfect orders
  - **Success criteria:**
    - Correct documentation
    - On-time processing
    - Accurate fulfillment
    - Compliance adherence

These metrics provide coverage of:

- System performance
- Business outcomes
- Automation effectiveness
- Risk management
- Operational excellence

Siloed data

Siloed data is a major challenge faced by many companies' supply chain operations. Data exists separately and is not accessible by other departments or business unit. As a result, decision making is made at each local level while lacking upstream and downstream indicators that would drive improved supply chain execution and risk mitigation.

A *data fabric* alleviates the frustration of hunting through data across multiple systems by creating a unified data architecture that supply chain teams can quickly access and trust. End users from procurement specialists to logistics managers can find, analyze, and act on real-time information through intuitive interfaces, replacing manual data gathering with automated insights. Further, by combining data across areas of the supply chain, leading indicators and downstream results can be correlated for greater performance management and risk avoidance.

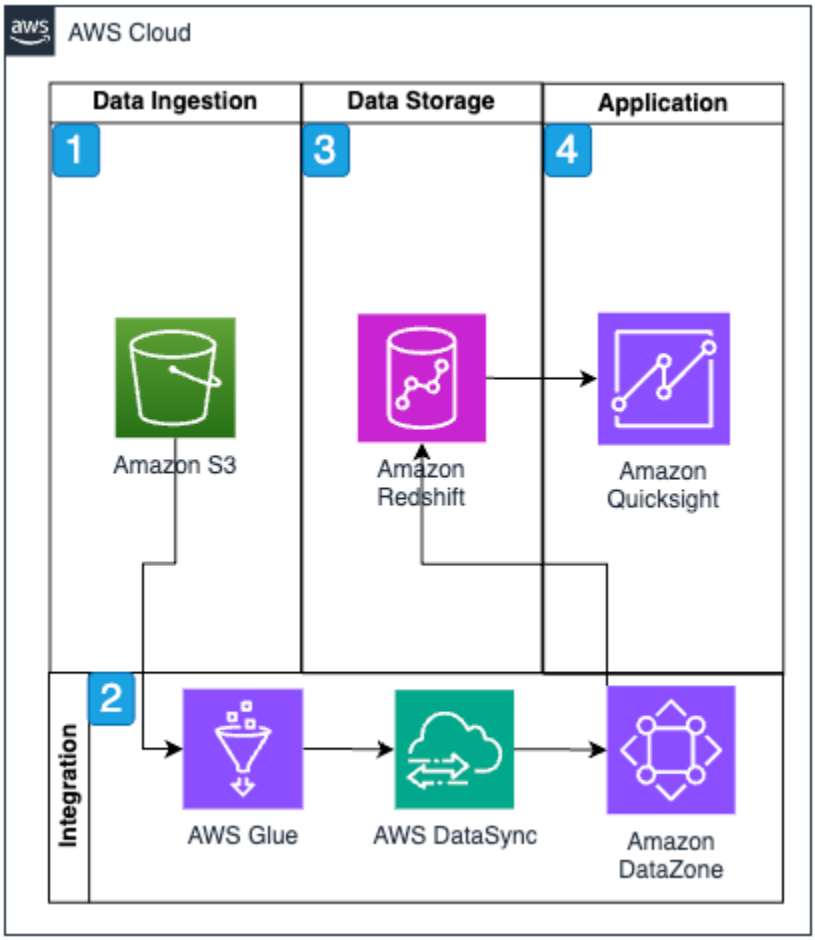
Implementing a data fabric in the supply chain using the AWS Well-Architected Framework delivers self-service access to reliable data while maintaining enterprise-grade security and performance. Business analysts can directly connect to data from IoT devices, ERP systems, and external feeds

through AWS services including Amazon S3 for storage, AWS Glue for ETL processing, and AWS DataSync for data movement and synchronization.

The Well-Architected Framework pillars provide users confidence as they follow efficient standards. Security controls protect sensitive data while allowing appropriate access. Reliability features help prevent disruptions to daily operations. Cost optimization keeps data storage and processing economical. Operational excellence means systems run smoothly without IT intervention. Performance efficiency delivers fast query responses and real-time analytics capabilities.

Supply chain teams gain powerful analytics capabilities through the data fabric. Business analysts run complex queries in Amazon Redshift. Planners and managers create their own visualizations and reports in Quick Suite without waiting for IT support. These self-service tools enable predictive analytics, process optimization, and data-driven decisions across roles. The result is greater productivity, faster response times, and better outcomes through accessible, trusted data and analytics.

Reference architecture



Architecture description

1. Ingest data from external and internal systems into Amazon S3.
2. AWS Glue provides integration data flows. AWS DataSync to migrate data from on premises to AWS Cloud. Amazon DataZone to catalog and provide fine grained control of the data being integrated.
3. Amazon Redshift provides the structured data store.
4. For the application layer, Amazon Quicksight provides dashboards, reporting, and analytics.

Architecture objectives

- Data accessibility and unification
- Operational analytics
- Business user empowerment
- Supply chain performance enhancement
- Operational efficiency
- Data quality and trust

Metrics

Based on the given data fabric and AWS Well-Architected Framework scenario, the relevant metrics that provide valuable insights for measuring success and performance are:

- Data accuracy:
  - **Metric**: Percentage of accurate data transfers.
  - **Rationale**: Critical for supply chain operations where data quality directly impacts decision-making.
  - **Well-Architected pillar**: Reliability.
  - Aligns with the need for trusted data.

- System downtime:
  - **Metric**: System uptime percentage.
  - **Rationale**: Essential for maintaining continuous access to real-time supply chain data.

  - **Well-Architected pillar**: Reliability.
  - Critical for supporting uninterrupted supply chain operations.

- Response time:
  - **Metric**: Average response time.
  - **Rationale**: Crucial for real-time analytics and quick decision-making.
  - **Well-Architected pillar**: Performance efficiency.
  - Important for self-service analytics mentioned in the scenario.

- Security:
  - **Metric**: Number of security incidents and compliance adherence.
  - **Rationale**: Essential for protecting sensitive supply chain data.
  - **Well-Architected pillar**: Security.
  - Critical for maintaining enterprise-grade security mentioned in the scenario.

Supply chain command center (SC3)

Global enterprises today face critical gaps in their supply chain systems that hamper visibility, coordination, and responsiveness across their operations. These gaps often manifest as disconnected data silos, manual intervention requirements, and the inability to adapt quickly to market changes or disruptions. Legacy systems, while robust in their core functions, frequently lack the agility and intelligence needed to manage modern supply chain complexities, leading to inefficiencies, increased costs, and missed opportunities for optimization.

Amazon SC3 provides capabilities to addresses these gaps in the end-to-end (E2E) supply chain. Organizations can either fully implement the SC3 as a stand-alone application or integrate its microservices with existing supply chain systems to coordinate operations. This flexible approach enables real-time decision-making for optimal resource allocation and workload balancing.

SC3 uses AWS's advanced AI and generative AI capabilities, including Amazon Bedrock and custom machine learning models, to automatically cleanse and standardize product master data across enterprise systems. The solution's intelligent algorithms identify duplicate SKUs by analyzing product descriptions, specifications, and attributes, even when items are listed with different naming conventions or in multiple languages.

Using natural language processing and similarity matching, SC3 can detect and consolidate redundant product entries, flag obsolete items based on usage patterns, and correct inaccurate specifications through cross-referencing with vendor catalogs and industry databases.

For example, when analyzing maintenance parts data, the system might recognize that 1/2-inch steel bolt - zinc plated and Zinc-coated steel bolt 12.7mm refer to the same item, automatically suggesting consolidation while maintaining traceability of historical transactions. This automated data cleansing not only helps prevent erroneous purchase orders but also enables strategic sourcing opportunities by providing clear visibility into consolidated vendor spend, resulting in cost savings through improved vendor negotiations and reduced administrative overhead.

SC3 transforms spare parts management by combining predictive maintenance capabilities with intelligent inventory optimization. SC3 employs Amazon SageMaker AI machine learning algorithms to analyze equipment sensor data, maintenance histories, and usage patterns to forecast potential failures and automatically trigger parts ordering at optimal times.

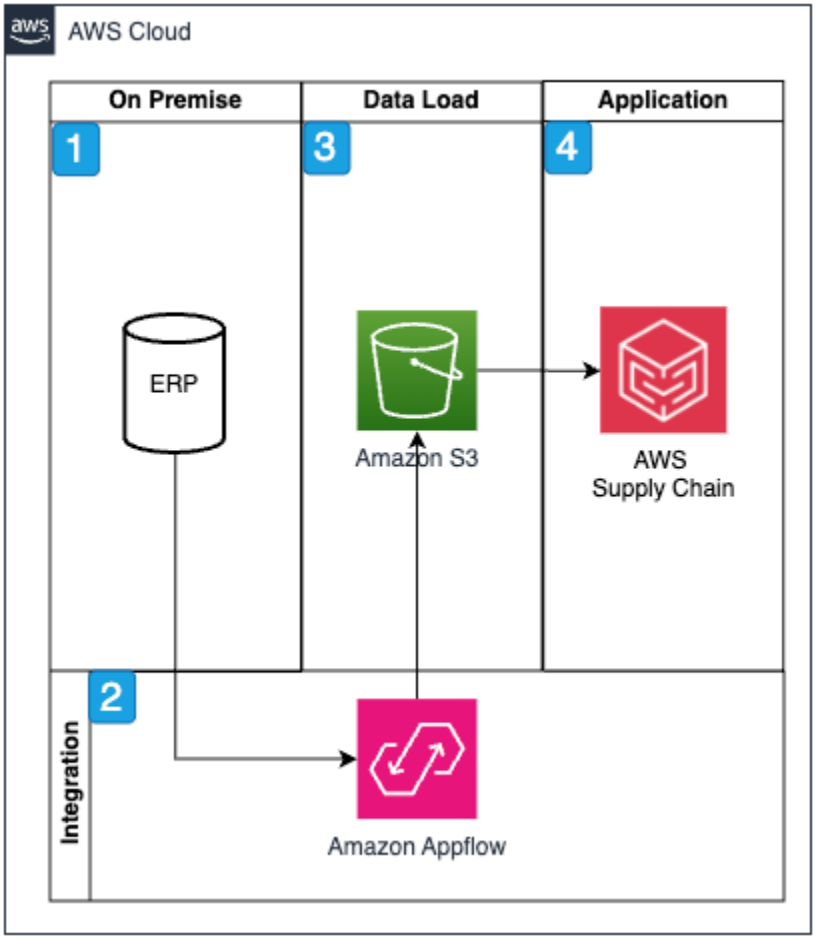
This predictive approach allows organizations to reduce working capital tied up in excess inventory while maintaining high service levels. For example, SC3 can integrate with equipment IoT sensors to monitor component wear, environmental conditions, and performance metrics, automatically adjusting safety stock levels based on predicted failure rates and lead times.

The system also considers factors such as part criticality, replacement costs, and downstream impact of equipment failure to optimize stocking strategies across multiple locations. By synchronizing maintenance schedules with parts availability and technician resources, SC3 helps organizations minimize both planned and unplanned downtime while reducing inventory carrying costs.

Quality control and compliance management gaps are resolved through SC3's AI/ML capabilities, which can be deployed either as a comprehensive solution or as targeted microservices. The system analyzes data from quality inspection stations, temperature sensors in storage or transit, and production line monitoring systems to identify potential quality issues before they impact downstream operations.

Organizations can implement SC3 for automated hold orders, inventory rerouting, stock recalls and replenishment from recall, automated notifications, and root cause analysis workflows.

Reference architecture



Architecture description

1. Ingest data from internal or external systems into Amazon S3 for loading into Amazon Redshift.
2. AWS Glue and AWS Glue DataBrew convert the raw data from Amazon S3 into Amazon Redshift for application access, queries, and dashboards.
3. Amazon SageMaker AI provides AI/ML for data management, analysis, decision support, and recommendations.
4. Amazon Amplify provides the front-end user experience. AWS Step Functions manage automated process flows. Amazon Location Services provides map-based visualizations. AWS Lambda holds business Logic. Amazon Quicksight provides dashboards and metrics.

Architecture objectives

- Enable near real-time updates to supply chain visibility and decision making across multiple parties.
- Scalable data ingestion and management.
- Automate data governance and cleansing using AI/ML.
- Enhance quality control through automated, standardized processes.
- Provide flexible deployment options as a complete solution or select microservices to support existing systems.

Metrics

Based on the supply chain command center (SC3) scenario, relevant metrics for an AWS Well-Architected Framework analysis are:

- Incident response time:
  - **Primary metric**: Time taken to detect, respond to, and resolve supply chain disruptions.
  - **Supporting metrics**:
    - Mean Time to Detect (MTTD) supply chain anomalies
    - Mean Time to Resolve (MTTR) critical issues
    - Percentage of incidents automatically resolved without human intervention
    - **Relevance**: Critical for measuring SC3's effectiveness in handling supply chain disruptions and maintaining business continuity, especially given its role in predictive maintenance and quality control

- Automation rate:
  - **Primary metric**: Percentage of supply chain tasks and processes that are fully automated.
  - **Supporting metrics:**
    - Number of manual interventions required per week
    - Percentage reduction in manual data entry tasks
    - Time saved through automated processes
    - **Relevance**: Directly measures SC3's core value proposition of automating supply chain operations and reducing manual intervention

- Resource utilization:
  - **Primary metric**: Percentage of available computing resources utilized during peak operations
  - **Supporting metrics**:
    - API response times under load
    - Database query performance
    - ML model inference latency
    - **Relevance**: Essential for SC3's scalability and cost-effectiveness, particularly important given the system's heavy reliance on AI/ML processing

- Compliance adherence:
  - **Primary metric**: Percentage of workflows that meet regulatory and quality control requirements
  - **Supporting metrics:**
    - Number of compliance violations detected and prevented
    - Percentage of quality control checks automated
    - Completeness of audit trails for regulated processes
    - Time to generate compliance reports
    - **Relevance**: Essential for measuring SC3's effectiveness in maintaining quality control and regulatory compliance, particularly important given the system's role in automated quality management and parts tracking

These metrics were selected because they:

- Align directly with SC3's core objectives of automation and efficiency
- Focus on critical aspects of system reliability and performance
- Provide actionable insights for optimization
- Align with regulatory and quality control objectives
- Support the AWS Well-Architected Framework's pillars (particularly operational excellence, performance efficiency, and cost optimization)

Warehouse automation and optimization (WAO)

Modern warehouse operations face unprecedented challenges in meeting the demands of e-commerce growth, labor constraints, and customer expectations for rapid delivery. Drawing from Amazon's extensive experience in operating over 150 million square feet of fulfillment center space globally, the Amazon Global Engineering team has developed proven approaches for warehouse automation and optimization. These insights, combined with AWS Cloud capabilities, form the foundation of the warehouse automation and optimization (WAO) offering from AWS Professional Services, providing customers with battle-tested solutions for their warehouse operations.

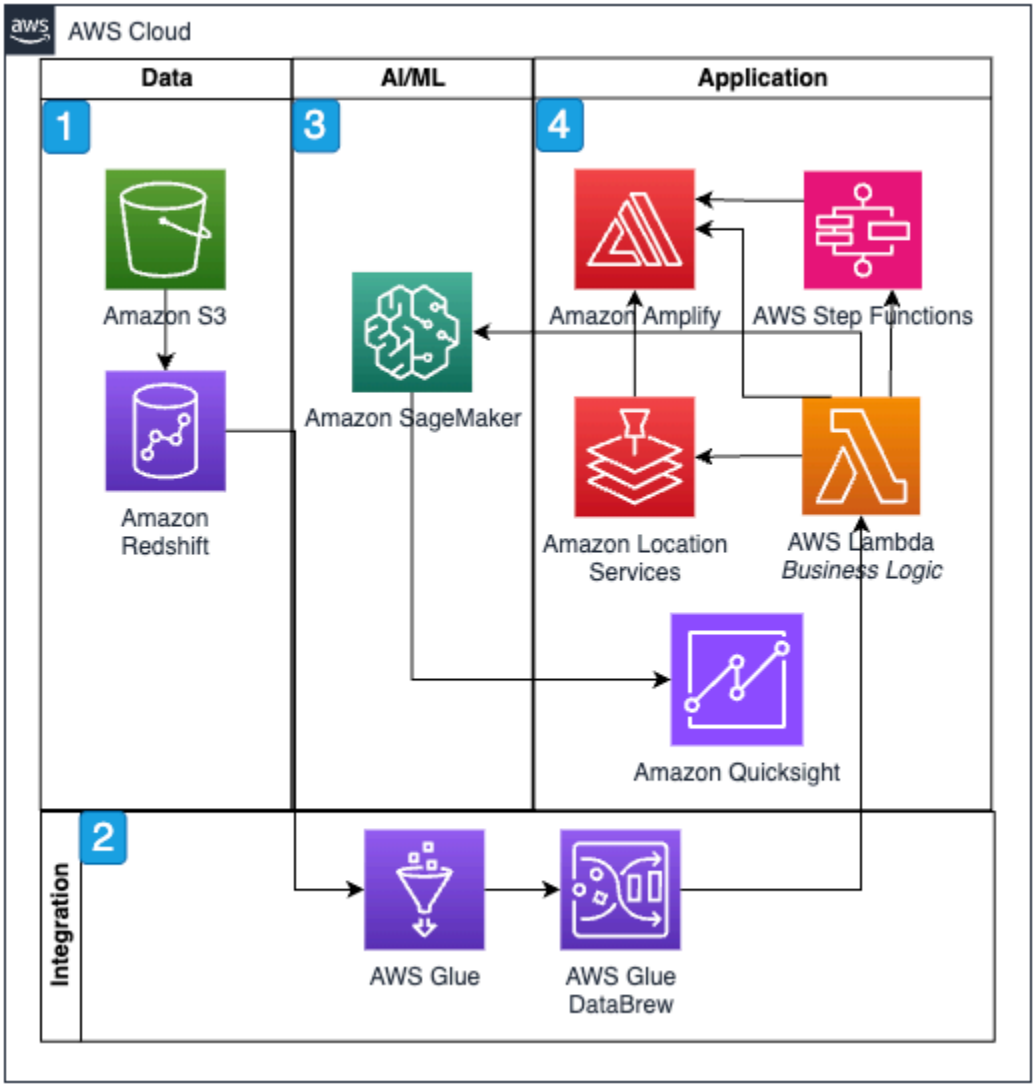
WAO uses multiple AWS services for physical facility design and simulation. Special cameras take images plus create dimensional data for 2D models of the facility that are fed through visualization GenAI services to transform into 3D, realistic models of operations. The three-dimensional models enable sophisticated scenario analysis by simulating various throughput calculations, thereby generating actionable insights for strategic decision-making. Real-time visualization of warehouse operations and KPIs can then be integrated with the model using AWS IoT Core to connect and sensors and automated systems throughout the facility. AWS IoT SiteWise creates a digital twin of the warehouse for monitoring and optimization. Amazon S3 and Amazon RDS store facility layouts, operational data, and simulation results. These simulation models validate design changes and predict operational impacts, for strategically laying out warehouses to maximize efficiency.

For automation and robotics integration, WAO employs AWS RoboMaker to develop, test, and deploy robotics applications, while AWS IoT Greengrass enables local compute and machine learning at the edge for automated guided vehicles (AGVs) and robotic picking systems. Amazon SageMaker AI powers ML models for demand forecasting, inventory optimization, and predictive maintenance. Real-time data processing is handled through Amazon Kinesis Data Streams and Amazon MSK, feeding into Amazon EMR for large-scale data processing. Amazon EventBridge orchestrates workflows between warehouse management systems, while AWS Step Functions manages complex automation sequences.

The solution's integration layer utilizes Amazon API Gateway and AWS AppSync to connect various warehouse systems and external applications. Security is maintained through AWS Identity and Access Management and AWS Security Hub, for proper access controls and compliance. Amazon CloudWatch and AWS X-Ray provide comprehensive monitoring and troubleshooting capabilities. The entire solution is deployed and managed using AWS CloudFormation and AWS Systems Manager, enabling consistent implementation across multiple facilities. This comprehensive technology stack, combined with expert advisory consulting from AWS Professional Services,

delivers a modern, efficient warehouse operation that reflects Amazon's own journey in warehouse innovation and excellence.

Reference architecture



Architecture description

1. Raw data is stored in Amazon SFormatted data is stored in Amazon RDS.
2. Amazon API Gateway provides endpoints for inbound data which is translated and loaded through AWS AppSync. Amazon Kinesis Firehose processes real-time data from IoT devices.
3. AWS IoT Core, AWS IoT SiteWise, and AWS IoT Greengrass provide the system for managing IoT devices. AWS RoboMaker provides the environment to build, test, and deploy robotics applications.

4. Amazon SageMaker AI provides AI/ML for measuring throughput and optimization recommendations. AWS Step Functions and Amazon EventBridge coordinate event driven process flows. AWS Lambda holds programming logic. Amazon Quick Suite presents dashboards and metrics.

Architecture objectives

- Physical design and simulation.
- Automation of operational IoT workflows.
- Data and analytics for warehouse operations.
- Integration of IoT operations and warehouse systems.

Metrics

Based on the warehouse automation and optimization (WAO) scenario, five relevant metrics are:

- Throughput efficiency:
  - **Primary metric:** Orders processed per hour compared to theoretical maximum
  - **Supporting metrics:**
    - Pick rate per automated system
    - Order fulfillment cycle time
    - Cross-dock processing speed – mainly applicable in retail operations where ocean containers are broken down for over the road transportation
    - **Relevance:** Directly measures the core operational efficiency of the automated warehouse

- Robotics performance:
  - **Primary metric:** Robot utilization rate and efficiency
  - **Supporting metrics:**
    - AGV navigation accuracy
    - Robot picking success rate
    - Mean time between robotic system failures
    - Automated task completion rates

    - **Relevance**: Critical for measuring the effectiveness of the robotics integration using AWS RoboMaker

- Digital twin accuracy:
    - **Primary metric:** Percentage variance between digital twin predictions and actual operations
    - **Supporting metrics:**
        - IoT sensor data accuracy
        - Simulation model precision
        - Real-time synchronization latency
        - Prediction accuracy of operational changes
        - **Relevance**: Essential for validating the AWS IoT SiteWise implementation and simulation reliability

- Edge computing performance:
    - **Primary metric:** Edge processing latency for critical operations
    - **Supporting metrics:**
        - AWS IoT Greengrass processing times
        - Local ML inference speed
        - Edge-to-cloud synchronization efficiency
        - Resource utilization at edge locations
        - **Relevance:** Crucial for real-time operation of automated systems

- System integration health:
    - **Primary metric:** End-to-end system integration uptime
    - **Supporting metrics:**
        - API response times
        - Inter-system communication latency
        - Event processing success rate
        - Integration error frequency
        - **Relevance:** Measures the effectiveness of the complex integration between various AWS services and warehouse systems

These metrics were selected because they:

- Focus on critical aspects of warehouse automation and performance
- Cover both physical and digital aspects of the solution
- Align with key AWS services used in the implementation
- Support measurement of operational excellence and efficiency
- Enable proactive monitoring and optimization of the warehouse automation system

Transportation visibility and fleet tracking

Today's complex supply chains require end-to-end visibility to manage disruptions, optimize delivery scheduling, and meet customer expectations for real-time tracking information. Transportation visibility and fleet tracking services have become essential for logistics providers to maintain competitive advantage and service levels. AWS provides a comprehensive set of services enabling organizations to achieve real-time visibility, optimize last-mile delivery operations, and enhance customer experience.

AWS Location Services enable critical transportation visibility through integration of two applications: a driver appointment scheduling interface and a mobile tracking application. Key workload requirements include real-time location tracking, dynamic task assignment, direct driver communication channels, and automated geofencing capabilities. The solution connects with mobile devices, processes location data streams, and delivers instant notifications to multiple stakeholders.

This architecture uses AWS managed services to deliver a scalable, reliable tracking solution. At its foundation, Amazon Location Services provides the core mapping and tracking functionality essential for fleet management and route visualization. AWS IoT Core serves as the backbone for secure device connectivity, enabling real-time data streaming from vehicles and mobile devices across the transportation network. The backend services for appointment scheduling and notification delivery are powered by Amazon API Gateway and AWS Lambda, for responsive and scalable processing of logistics operations. To support cross-system compatibility and enhance user experience, the mobile applications are built using AWS Amplify, providing a seamless interface for both drivers and dispatchers.

The implemented solution delivers comprehensive transportation visibility through multiple integrated capabilities. Real-time vehicle tracking and location monitoring provide constant

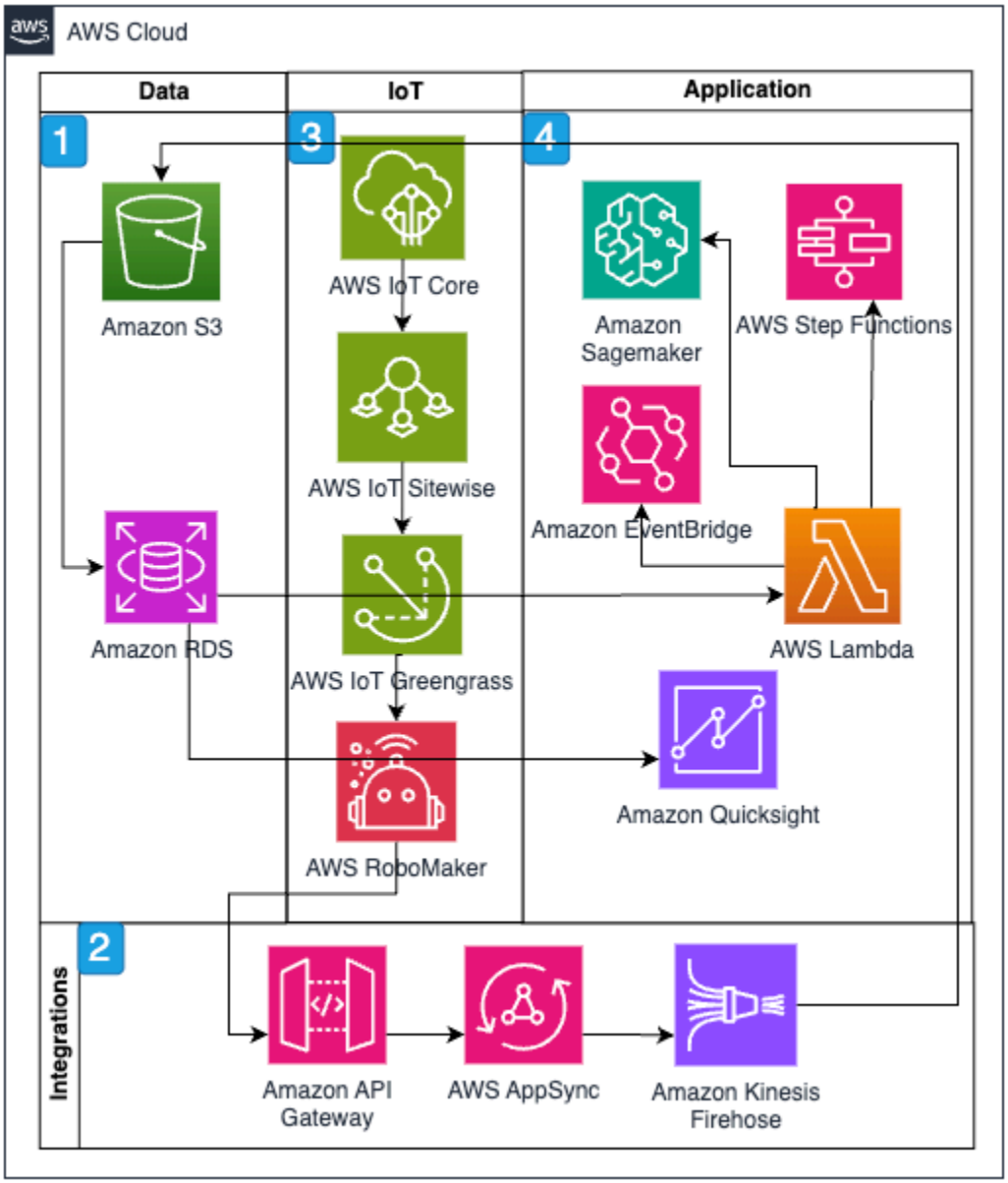
awareness of fleet positions, while automated geofence creation and breach notifications enable proactive management of delivery zones and waypoints. Dynamic route optimization and task assignment capabilities facilitate efficient resource utilization and adapt to changing conditions throughout the day. The solution includes robust in-app driver communication capabilities, facilitating direct coordination between drivers, dispatchers, and support teams. Additionally, customer-facing delivery status updates and ETAs enhance the end-customer experience by providing transparent and accurate delivery information. These combined features create a unified system that optimizes transportation operations while maintaining high service levels and customer satisfaction.

AWS services can seamlessly integrate with third-party Electronic Logging Device (ELD) solutions to create a comprehensive fleet management and route optimization system. ELD devices, which are mandated for commercial vehicles to track Hours of Service (HoS) compliance, connect to the vehicle's engine control module to collect critical data including driving time, rest periods, engine health, and fuel consumption. This data is ingested into AWS through Amazon API Gateway or AWS IoT Core, which provides secure device connectivity and message routing. Amazon Kinesis Data Streams processes the real-time ELD data streams alongside GPS locations, while Amazon S3 stores the historical compliance records and vehicle diagnostics.

The route optimization engine incorporates HoS constraints from the ELD data to make sure routes comply with driver work limits and required break periods. AWS Lambda functions monitor ELD alerts and driver status changes, triggering route adjustments through Amazon EventBridge when needed. Amazon DynamoDB maintains current driver status and available hours, while Quick Suite provides fleet managers with compliance dashboards and driver performance analytics. Amazon SageMaker AI models can analyze the combined ELD and route data to optimize driver assignments and predict maintenance needs based on engine diagnostics. This integrated solution supports regulatory compliance while maximizing fleet efficiency, with Amazon CloudWatch monitoring the entire system and Amazon SNS delivering critical alerts to fleet managers when compliance issues or vehicle problems are detected.

These capabilities result in improved operational efficiency, enhanced customer satisfaction, and optimized last-mile delivery performance. The solution's scalable architecture facilitates reliable performance during peak delivery periods while maintaining cost efficiency during normal operations.

Reference architecture



Architecture description

1. Amazon S3 holds raw data before it's loaded into Amazon DynamoDB.
2. Integration services include Amazon API Gateway and AWS AppSync for managing API endpoints. Amazon SNS provides notifications. Amazon Kinesis Data Streams processes near real-time data feeds for transportation assets.
3. AWS IoT Core in conjunction with Amazon Location Services combines the field device locations with maps for visibility.

4. Front end application is built in AWS Amplify using Amazon Sagemaker for AI/ML recommendations, AWS Lambda for business logic, Amazon EventBridge for routing and managing events, and Amazon Quicksight for presenting metrics or dashboards.

Architecture objectives

- Near real-time fleet tracking
- Route optimization
- Electronic logging device (ELD) compliance monitoring
- Drive communication
- Customer delivery updates
- Analytics and reporting

Metrics

Based on the transportation visibility and fleet tracking scenario, the four most relevant metrics are:

- Real-time tracking accuracy:
  - **Primary metric:** Location data accuracy and update frequency
  - **Supporting metrics:**
    - GPS position accuracy
    - Location update latency
    - Geofence detection reliability
    - Signal coverage percentage
    - **Relevance**: Core functionality for fleet visibility and customer tracking

- ELD compliance performance:
  - **Primary metric:** Hours of service (HoS) compliance rate
  - **Supporting metrics:**
    - Driver violation incidents
    - Rest period adherence
    - Data logging reliability

    - Compliance reporting accuracy
    - **Relevance**: Critical for regulatory compliance and driver safety

- Route optimization efficiency:
    - **Primary metric:** Delivery efficiency improvement percentage
    - **Supporting metrics:**
        - Fuel consumption reduction
        - On-time delivery rate
        - Route completion time
        - Distance per delivery
        - **Relevance**: Measures operational efficiency and cost savings

- System integration reliability:
    - **Primary metric:** End-to-end system uptime and data flow reliability
    - **Supporting metrics:**
        - API response times
        - Device connectivity rates
        - Data synchronization success
        - Event processing latency
        - **Relevance**: Essential for maintaining continuous visibility and operations

These metrics were selected due to the following reasons:

- Focus on critical aspects of transportation visibility
- Address regulatory compliance requirements
- Measure operational efficiency improvements
- Evaluate system reliability and performance
- Support both technical and business objectives of the solution

Product traceability

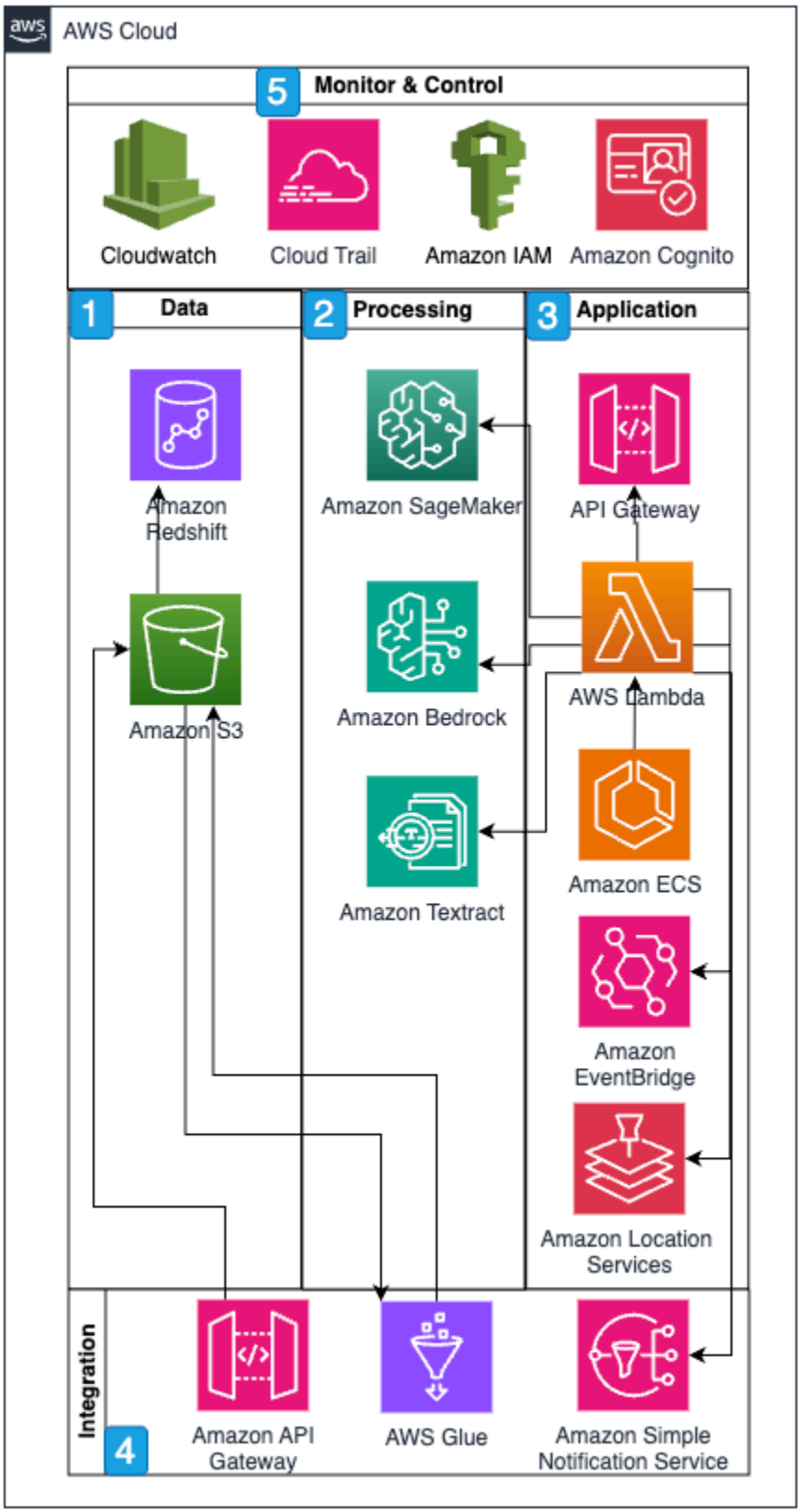
Product traceability in supply chain management is the ability to track and document the journey of products and their components from raw materials to finished goods. Effective traceability enables organizations to verify product authenticity, measure contractual obligations, facilitate quality control, manage recalls efficiently, and maintain regulatory compliance while providing transparency to stakeholders.

Product traceability addresses the critical need for visibility and validation of each party supporting a particular product's supply chain. Tracing products back up the supply chain involves frequent updates as there are changes in vendors, suppliers, warehouses, manufacturing, and carriers. Begin with AWS Glue, for seamless ingestion, cleaning, and processing of third-party data, particularly focused on vital information such as shipping and invoice details. A user-friendly, serverless portal, powered by Amazon Route 53, Amazon Cognito, Amazon CloudFront, and Amazon S3, enables stakeholders to upload supply chain certificates effortlessly.

The pivotal feature of this architecture lies in its meticulous data extraction process initiated by Amazon EventBridge and orchestrated by AWS Step Functions. Here, Amazon Textract's capabilities, including optical character recognition and plain language queries, facilitate the extraction of key details from certificates, such as expiration dates and certificate numbers. The inclusion of Amazon Location Service further enhances traceability by mapping supplier addresses to GPS coordinates, offering a visual representation of geographical locations. Notably, the system allows for optional crosschecking of the extracted data against third-party information, providing a validation mechanism crucial for the authenticity and accuracy of product traceability data.

Product traceability from AWS Professional Services is specifically tailored to meet the demands of global enterprises, offering a seamless, automated, and secure solution. Through a combination of data extraction, mapping, and validation processes, it provides organizations with a comprehensive toolset to achieve real-time visibility and accuracy in tracing activities throughout the supply chain.

Reference architecture



Architecture description

1. Data is stored in Amazon S3 for processing into Amazon Redshift for the data lake.
2. Processing through Amazon SageMaker AI ML models and AI services
3. Real-time analysis and prediction
4. API-based service delivery
5. Continuous monitoring and optimization

Architecture objectives

- Scalable processing of supply chain data
- Automated document processing
- Real-time insights and predictions for end-to-end supply chain
- Audit compliance and secure data interchange
- Integration with existing systems, internal and external
- Monitoring and optimization capabilities

Metrics

Based on the product traceability scenario, the three relevant metrics are:

- Data accuracy and validation:
  - **Primary metric:** Accuracy rate of extracted and validated product data
  - **Supporting metrics:**
    - Document extraction success rate
    - Data validation match rate
    - Certificate verification accuracy
    - Error detection rate in supply chain documentation
    - **Relevance**: Critical for reliable traceability and compliance verification

- Traceability response time
  - **Primary metric:** Time to trace a product's complete supply chain journey

- **Supporting metrics:**
  - Data retrieval speed
  - Certificate processing time
  - Query response time for product history
  - Time to generate traceability reports
  - **Relevance:** Essential for rapid response to quality issues or recalls

1. Data integration completeness:
   - **Primary metric:** Percentage of supply chain events successfully captured and linked
   - **Supporting metrics:**
     - Supply chain visibility coverage
     - Partner data integration rate
     - Documentation completeness score
     - Chain of custody gaps identified
     - **Relevance:** Measures the effectiveness of end-to-end traceability

These metrics were selected because they:

- Focus on core traceability requirements
- Address key compliance and quality control needs
- Measure system effectiveness in maintaining complete chain of custody
- Align with regulatory and stakeholder requirements
- Support rapid response capabilities for quality issues or recalls

Scenario summary

The AWS Well-Architected Framework provides a comprehensive foundation for building resilient, efficient, and secure supply chain solutions across industries. These eight scenarios demonstrate how organizations can use AWS services to address critical supply chain challenges while maintaining architectural excellence across all pillars.

From planning and operations to product traceability, these architectures showcase how AWS technologies enable digital transformation of supply chains through:

- **Intelligent automation:** Using AI/ML services like Amazon SageMaker AI and Amazon Bedrock to automate manual processes, enhance decision-making, and optimize operations
- **Enhanced visibility:** Creating unified views across the supply chain through data fabric architectures and command center capabilities
- **Improved collaboration:** Enabling secure information sharing and coordination between partners through cloud applications
- **Operational resilience:** Building reliable and scalable solutions that can adapt to disruptions and changing business needs
- **Cost efficiency:** Optimizing resource utilization while maintaining performance through cloud architectures

The scenarios provide blueprints for organizations to modernize their supply chains while adhering to architectural best practices. Whether implementing individual components or complete solutions, the Well-Architected Framework makes sure these transformations deliver business value while maintaining security, reliability, and operational excellence.

As supply chains continue to evolve, these architectures demonstrate AWS' commitment to helping organizations build future-ready solutions that can scale and adapt to new challenges. Through the Well-Architected Framework, organizations gain both the technical foundation and architectural guidance needed to succeed in today's dynamic supply chain landscape.

Operational excellence

The operational excellence pillar provides guidance on running and monitoring systems to deliver business value and continually improving supporting processes and procedures.

The operational excellence pillar includes the ability to support development and run workloads effectively, gain insight into their operations, and to continuously improve supporting processes and procedures to deliver business value.

This section provides an overview of design principles, questions, best practices, and implementation guidance on implementation. For more information, see the Operational Excellence Pillar whitepaper.

Focus areas

- Design principles
- Organization
- Operate
- Evolve
- Resources

Design principles

- Establish clear, measurable, and regularly reviewed key performance indicators (KPIs) across the entire supply chain to drive data-informed decisions and foster continuous improvement.
- Empower supply chain teams with the necessary data, tools, and authority to make real-time, autonomous decisions that optimize operations and respond rapidly to dynamic conditions.
- Prioritize and integrate artificial intelligence (AI) strategically within the supply chain, facilitating clear understanding of roles, responsibilities, and organizational structures to maximize AI-driven outcomes.
- Implement robust processes for assessing and managing the operational readiness of new partners and for the comprehensive management and resolution of operational issues, including the validation of corrective actions.
- Design and operate the supply chain application with inherent mechanisms to meet all relevant compliance and regulatory requirements.

- Foster a culture and implement mechanisms for continuous evolution and adaptation of supply chain operations to use emerging technologies, best practices, and market dynamics.

Organization

SCOPS01: How do you identify and track all stakeholders interacting with the supply chain application?

To assess the impact of outages and develop robust business continuity plans, it is important to understand who the end users of the application are and how they use it today.

SCOPS02: How are key performance indicators established, regularly reviewed, and communicated for each stage of the supply chain?

The ability to measure and understand the health and effectiveness of your supply chain operations is critical across all stages.

SCOPS03: How do you empower supply chain teams to make real-time decisions to optimize operations?

The agility and responsiveness of supply chain teams in modern supply chains is important for making informed and timely decisions.

SCOPS04: How do you determine priorities for integrating AI into your supply chain?

Determining priorities for AI integration in your supply chain is a critical strategic decision that impacts operational efficiency, cost management, and competitive advantage.

SCOPS05: How do you determine if everyone's part in enabling business success with AI is understood?

Understanding everyone's role in enabling AI success is crucial because it establishes clear accountability, facilitates proper resource allocation, and creates organizational alignment across technical and business functions.

SCOPS06: How do you structure your organization to support AI-driven supply chain outcomes?

Properly structuring your organization to support AI-driven supply chain outcomes is critical because it determines how effectively you can implement, scale, and derive value from AI technologies across your supply chain operations.

SCOPS07: How do you meet the compliance and regulatory needs for your supply chain workload?

Meeting compliance and regulatory requirements for your supply chain workload is essential because non-compliance can result in significant legal penalties, operational disruptions, and reputational damage across global markets.

SCOPS08: How do you assess and manage the operational readiness of new suppliers or logistics partners?

Assessing and managing the operational readiness of new suppliers or logistics partners is crucial because these third parties directly impact your ability to deliver products reliably, maintain quality standards, and respond to market changes.

SCOPS09: How do you facilitate continuous refresh of your demand and supply data?

Facilitating continuous refresh of demand and supply data is critical because it enables real-time visibility and decision-making across your supply chain, allowing for faster responses to market changes and operational disruptions.

Best practices

- SCOPS01-BP01 Identify and track all stakeholders interacting with the supply chain application
- SCOPS02-BP01 Define, monitor, and communicate KPIs across the entire supply chain
- SCOPS03-BP01 Provide supply chain teams with access to real-time data, analytics, and decision-making tools
- SCOPS04-BP01 Prioritize AI integration based on business value, feasibility, and alignment with strategic supply chain objectives
- SCOPS05-BP01 Establish clear roles, responsibilities, and communication channels for all stakeholders involved in AI-driven initiatives
- SCOPS06-BP01 Establish an org that fosters collaboration, data-driven decision-making, and continuous innovation in AI-driven operations
- SCOPS07-BP01 Implement processes and technologies for continuous compliance with regulations, data privacy laws, and internal policies
- SCOPS08-BP01 Implement a process for assessing, onboarding, and monitoring the operational readiness of new suppliers and logistics partners
- SCOPS09-BP01 Automate integrated data pipelines for real-time demand and supply data refresh across the supply chain

SCOPS01-BP01 Identify and track all stakeholders interacting with the supply chain application

Create a comprehensive inventory of all stakeholders who interact with the supply chain application. This includes internal users (like employees and departments), external partners (like suppliers and customers), and any third-party services integrated with the application. Document how each stakeholder group uses the application.

This involves understanding their workflows, frequency of access, critical functions they perform, and dependencies on the application. Assess the impact of potential outages on each stakeholder group. This can be done through impact analysis workshops, surveys, or historical data analysis.

Establish communication channels to regularly engage with stakeholders. This makes sure that their needs and pain points are continuously captured and addressed.

Implement monitoring solutions to track stakeholder interactions with the application in real-time. This can involve usage analytics, logging, and feedback mechanisms.

Desired outcome: Up-to-date map of all stakeholders interacting with the supply chain application including detailed information about each stakeholder's role, responsibilities, access levels, and usage patterns.

Benefits of establishing this best practice:

- Enhances the organization's ability to respond swiftly and effectively to outages or disruptions, minimizing downtime and reducing the potential for supply chain bottlenecks.
- Fosters better communication and collaboration among stakeholders, leading to improved overall satisfaction and engagement.
- Provides valuable data for analyzing usage patterns and identifying areas for optimization, contributing to continuous improvement in supply chain operations.
- Supports the development of comprehensive business continuity plans, making sure that the organization is well-prepared to handle unforeseen events and maintain operational excellence in the cloud.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Gather detailed insights on which persona is accessing the supply chain application. This could include documenting user access patterns such as typical operating hours, role-based rights and privileges within the application, and network access methods including internet, VPN, or private connectivity. Establishing comprehensive stakeholder mapping enables organizations to understand dependencies and optimize system performance based on actual usage patterns.

Implementation steps

1. Conduct interviews and surveys with end-users to identify all personas.
2. Document user access patterns, roles, and network access methods.
3. Create a stakeholder map that outlines the relationships and dependencies.

SCOPS02-BP01 Define, monitor, and communicate KPIs across the entire supply chain

To effectively manage and optimize your supply chain, it's crucial to establish a comprehensive set of KPIs that span from demand planning through to final delivery. These KPIs should be carefully selected to align with business objectives and provide actionable insights. Regular monitoring of these KPIs, ideally through interactive dashboards, allows for real-time performance assessment. Furthermore, consistent and transparent communication of KPI results to all relevant stakeholders fosters accountability and makes sure everyone is working towards shared goals, ultimately leading to improved operational efficiency, enhanced decision-making, and better alignment of supply chain activities with overall business strategy.

Desired outcome: A clear, data-driven understanding of supply chain performance at every stage, enabling proactive identification of issues and continuous improvement.

Benefits of establishing this best practice:

- Improved operational efficiency and effectiveness.
- Enhanced decision-making capabilities based on real-time data.
- Increased accountability and performance ownership across supply chain teams.
- Better alignment of supply chain activities with business goals.
- Proactive identification and mitigation of potential disruptions.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

- Collaborate with supply chain managers and team leads to define relevant KPIs for their respective areas, utilizing business intelligence tools and data visualization systems to create interactive dashboards. Establish a regular cadence for KPI review meetings with clear ownership assignments to maintain accountability and continuous improvement across all supply chain stages.

Implementation steps

1. Identify key stages of your supply chain (for example, planning, sourcing, manufacturing, logistics, delivery).

2. For each stage, define a set of measurable KPIs that align with business objectives.
3. Implement data collection mechanisms to gather information for each KPI.
4. Develop dashboards and reports to visualize KPI performance.
5. Establish a regular review cycle for KPIs and communicate results to stakeholders.

SCOPS03-BP01 Provide supply chain teams with access to real-time data, analytics, and decision-making tools

Empowering supply chain teams hinges on providing them with immediate access to current and accurate information, coupled with the analytical capabilities to interpret it. This involves investing in robust supply chain management (SCM) software that offers real-time data integration, advanced analytics, and predictive modeling features.

Developing customized dashboards and reports makes sure that teams receive relevant insights tailored to their specific roles. Crucially, ongoing training and support are essential to make sure that teams are proficient in utilizing these tools and can confidently apply the insights gained to make swift and effective decisions, thereby enhancing operational efficiency, reducing costs, and improving resilience to disruptions.

Desired outcome: Supply chain teams are agile and responsive. They can make informed and timely decisions that optimize operations and mitigate disruptions.

Benefits of establishing this best practice:

- Faster response to changes in demand or supply.
- Improved operational efficiency and reduced costs.
- Enhanced customer satisfaction due to optimized delivery and service.
- Increased resilience to supply chain disruptions.
- More efficient resource allocation.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

- Invest in supply chain management software that offers real-time data integration and analytics capabilities, while developing custom dashboards and reports tailored to specific team needs.

Provide ongoing training and support to make sure teams are proficient in using these tools and can make data-driven decisions effectively.

Implementation steps

1. Assess current data visibility and identify gaps in real-time information.
2. Implement or upgrade SCM systems to enhance real-time data capture and integration.
3. Introduce analytics and predictive modeling tools relevant to supply chain operations.
4. Develop and deploy decision support systems for key operational areas.
5. Provide comprehensive training programs to supply chain teams on data interpretation and tool usage.
6. Establish clear guidelines and processes for real-time decision-making.

SCOPS04-BP01 Prioritize AI integration based on business value, feasibility, and alignment with strategic supply chain objectives

Strategic AI integration begins with a clear prioritization framework. This involves identifying potential AI use cases across the supply chain and then rigorously assessing each one based on its potential business value, technical feasibility, and the readiness of the underlying data. Forming a cross-functional team with representatives from IT, supply chain operations, and business leadership is crucial for this evaluation process.

By employing a scoring mechanism that considers business impact, feasibility, and strategic alignment, organizations can develop a clear, prioritized roadmap for AI initiatives. This approach makes sure that resources are efficiently allocated, leading to maximized ROI from AI investments and accelerated adoption of AI across the supply chain, ultimately contributing to improved decision-making and operational efficiency.

Desired outcome: A clear, prioritized roadmap for AI integration that maximizes business value and supports the evolution of an intelligent supply chain.

Benefits of establishing this best practice:

- Maximized ROI from AI investments.
- Targeted application of AI to address critical supply chain challenges.
- Efficient allocation of resources for AI development.

- Accelerated adoption of AI across the supply chain.
- Improved decision-making and operational efficiency through AI-driven insights.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

- Form a cross-functional team with representatives from IT, supply chain operations, and business leadership to evaluate AI opportunities and develop a framework for assessing initiatives based on defined criteria. Consider external consultants or AI specialists if internal expertise is limited to facilitate comprehensive evaluation of potential AI applications.

Implementation steps

1. Conduct workshops to identify potential AI use cases across the supply chain.
2. For each use case, assess potential business value, technical feasibility, and data readiness.
3. Prioritize AI initiatives based on a scoring mechanism that considers business impact, feasibility, and strategic alignment.
4. Develop a phased implementation roadmap, starting with pilot projects.
5. Secure necessary resources (budget, personnel, technology) for prioritized AI initiatives.

SCOPS05-BP01 Establish clear roles, responsibilities, and communication channels for all stakeholders involved in AI-driven initiatives

Successful integration of AI into the supply chain necessitates a workforce that fully comprehends and actively contributes to its success. This involves clearly defining roles and responsibilities for every stakeholder group impacted by AI, from data scientists to operational teams.

Establishing robust communication plans and conducting workshops is vital to educate employees on the role of AI, its impact on their functions, and new processes. Providing comprehensive training programs equips employees with the necessary AI-related skills.

Furthermore, creating feedback loops allows for continuous assessment of understanding and addresses concerns, fostering increased adoption, reduced resistance to change, and enhanced collaboration between human and AI capabilities.

Desired outcome: A workforce that understands and actively contributes to the success of AI-driven supply chain initiatives, leading to improved operational efficiency and business outcomes.

Benefits of establishing this best practice:

- Increased adoption and utilization of AI solutions.
- Reduced resistance to change and improved employee morale.
- Enhanced collaboration and synergy between human and AI capabilities.
- More effective utilization of AI to drive business value.
- A more skilled and adaptable workforce.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

- Conduct workshops and informational sessions to explain the role of AI in the supply chain and its impact on various job functions, while creating clear documentation outlining new processes and responsibilities related to AI tools.
- Encourage cross-functional teams to work together on AI projects to foster understanding and collaboration across different organizational areas.

Implementation steps

1. Identify all stakeholder groups impacted by AI integration in the supply chain.
2. Define specific roles and responsibilities for each group in the context of AI initiatives.
3. Develop and execute a communication plan to inform and educate stakeholders.
4. Implement training programs to equip employees with necessary AI-related skills.
5. Establish feedback loops to gauge understanding and address concerns.
6. Regularly communicate the impact and success of AI initiatives.

SCOPS06-BP01 Establish an org that fosters collaboration, data-driven decision-making, and continuous innovation in AI-driven operations

To truly realize the benefits of AI in the supply chain, an organization's structure must be purposefully designed to support it. This involves evaluating the current structure to identify and

remove potential barriers to AI integration. Defining new roles and reporting lines for AI-related functions, such as AI product owners or MLOps engineers, is crucial.

Establishing cross-functional teams for specific AI projects and implementing agile development processes for AI solutions can significantly accelerate development and deployment. Additionally, developing a robust data governance framework supports data quality and accessibility, which are fundamental to AI success.

By investing in training and upskilling programs, organizations can further enhance their ability to attract and retain AI talent, leading to greater agility and adaptability in response to market changes.

Desired outcome: An organizational structure that seamlessly integrates AI into supply chain operations, enabling efficient development, deployment, and ongoing optimization of AI-driven solutions.

Benefits of establishing this best practice:

- Accelerated development and deployment of AI solutions.
- Improved collaboration and knowledge sharing across functions.
- Enhanced ability to attract and retain AI talent.
- More efficient resource allocation for AI initiatives.
- Greater agility and adaptability in response to market changes.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

- Evaluate your current organizational structure to identify potential barriers to AI integration and Define roles and reporting lines for AI-related functions.
- Consider a hub-and-spoke model for AI, where a central Center of Excellence supports distributed teams across different supply chain functions.

Implementation steps

1. Assess the current organizational structure and identify areas for optimization to support AI.
2. Define new roles and responsibilities for AI-related functions (for example, AI product owner, MLOps engineer).

3. Establish cross-functional teams for specific AI projects.
4. Develop a data governance framework to maintain data quality and accessibility.
5. Implement agile development processes for AI solution creation.
6. Invest in training and upskilling programs for employees.

Prepare

SCOPS07-BP01 Implement processes and technologies for continuous compliance with regulations, data privacy laws, and internal policies

Maintaining continuous compliance in supply chain applications requires a multi-faceted approach. This begins with thoroughly identifying all relevant compliance frameworks and regulations and then conducting a gap analysis to pinpoint areas requiring attention.

Implementing necessary technical controls and process changes within the application, alongside developing a robust data governance and security framework, are crucial for protecting sensitive information.

Engaging legal and compliance experts is vital for guidance. Use cloud provider compliance certifications and integrate compliance checks into the application development lifecycle to streamline the process.

Furthermore, establishing a regular schedule for internal and external audits, providing continuous employee training on compliance best practices, and maintaining comprehensive documentation of all activities are essential for demonstrating adherence, reducing risks, and enhancing trust.

In the supply chain space, several compliance certifications demonstrate a commitment to various standards and best practices. These include:

- **ISO 9001:** This certification focuses on quality management systems and indicates a dedication to consistent, high-quality products and services.
- **ISO 14001:** This certification signifies adherence to environmental management standards, emphasizing sustainable practices and compliance with environmental regulations.
- **ISO 27001:** This certification relates to information security management systems, verifying legal compliance and safeguarding confidential data.
- **ISO 45001:** This certification focuses on occupational health and safety, facilitating a safe work environment for employees.

- **Business Social Compliance Initiative (BSCI):** This program emphasizes ethical labor practices and worker safety within global supply chains, especially relevant for businesses sourcing from developing countries.
- **Customs-Trade Partnership Against Terrorism (C-TPAT):** A voluntary program led by U.S. Customs and Border Protection (CBP) to improve supply chain security against terrorism, it involves rigorous risk assessment and implementation of security measures. C-TPAT certification allows for expedited processing and reduced examinations of cargo.
- **Food safety certifications:** These certifications, including HACCP, Safe Quality Food (SQF), and FSSC 22000, make sure that food products meet safety standards and quality requirements throughout the supply chain.
- **Sustainable Supply Chain Certifications:** These certifications, such as FSC chain of custody, Rainforest Alliance Sustainable Agriculture Standard, and Cradle to Cradle Certified, focus on environmental and social sustainability, ethical sourcing, and promoting a circular economy within the supply chain.
- **Cybersecurity Maturity Model Certification (CMMC):** This framework assesses and enhances the cybersecurity posture of companies in the defense industrial base, maintaining protection of sensitive information.

Desired outcome: A supply chain application that consistently adheres to all relevant compliance and regulatory mandates, minimizing legal risks and maintaining business integrity.

Benefits of establishing this best practice:

- Reduced risk of legal penalties, fines, and reputational damage.
- Enhanced trust with customers, partners, and regulatory bodies.
- Improved data security and protection of sensitive information.
- Streamlined audit processes and easier demonstration of compliance.
- Greater operational resilience and stability.

Level of risk exposed if this best practice is not established: High

Implementation guidance

- Engage legal and compliance experts to thoroughly review applicable regulations and
- Use cloud provider compliance certifications and services such as AWS Artifact.

- Integrate compliance checks into your application development lifecycle to verify continuous adherence to regulatory requirements throughout the development and deployment process.

Implementation steps

1. Identify all relevant compliance frameworks and regulations.
2. Conduct a gap analysis between current practices and regulatory requirements.
3. Implement necessary technical controls and process changes within the supply chain application.
4. Develop a robust data governance and security framework.
5. Establish a schedule for regular internal and external compliance audits.
6. Provide continuous training to employees on compliance best practices.
7. Maintain comprehensive documentation of all compliance activities.

SCOPS08-BP01 Implement a process for assessing, onboarding, and monitoring the operational readiness of new suppliers and logistics partners

Integrating new suppliers and logistics partners seamlessly into the supply chain is vital for maintaining operational efficiency and resilience. This requires a structured process that begins with clearly defining criteria for selecting and evaluating potential partners. A comprehensive onboarding program, including system integration and training, should be in place to facilitate a smooth transition. Conducting thorough operational readiness assessments before full engagement is crucial to verify their capabilities.

Furthermore, establishing performance KPIs and a regular monitoring schedule allows for continuous oversight of partner performance, while a formal review process verifies ongoing accountability. Utilizing supplier relationship management (SRM) software can help manage partner information and performance, leading to stronger relationships and enhanced contributions to the supply chain.

Desired outcome: Seamless integration of new suppliers and logistics partners into the supply chain with minimal disruption and assured operational capability.

Benefits of establishing this best practice:

- Reduced risks associated with new partner onboarding.
- Improved supply chain resilience and reliability.
- Enhanced partner performance and contribution to overall supply chain efficiency.
- Streamlined integration processes.
- Stronger relationships with key supply chain collaborators.
- **Level of risk exposed if this best practice is not established:** Medium

Implementation guidance

- Develop standardized checklists and evaluation criteria for assessing new partners, while utilizing supplier relationship management software to manage partner information and performance.
- Assign a dedicated team or individual to oversee the onboarding and ongoing management of new partners to maintain consistency and accountability.

Implementation steps

1. Define clear criteria for selecting and evaluating new suppliers and logistics partners.
2. Develop a structured onboarding program, including system integration and training.
3. Conduct thorough operational readiness assessments before full engagement.
4. Establish performance KPIs and a regular monitoring schedule.
5. Implement a formal review process for ongoing partner performance.

SCOPS09-BP01 Automate integrated data pipelines for real-time demand and supply data refresh across the supply chain

To achieve an agile and responsive supply chain, it is imperative to have access to up-to-date and accurate demand and supply data. This necessitates the implementation of automated and integrated data pipelines that can provide real-time or near real-time data refresh from all relevant sources, both internal and external.

Identifying current data flow bottlenecks and manual processes is the first step toward optimization. Investing in data integration tools and systems that support real-time processing, along with configuring real-time data streaming for critical datasets, is essential.

Establishing robust data validation, cleansing, and governance procedures maintains data quality. Regularly reviewing and optimizing these data refresh processes and technologies further enhances the accuracy of forecasts, optimizes inventory, and enables faster responses to disruptions and market fluctuations.

Desired outcome: Access to up-to-date and accurate demand and supply data, enabling agile planning, rapid response to market changes, and optimized inventory levels.

Benefits of establishing this best practice:

- Improved accuracy of demand forecasts and supply plans.
- Reduced lead times and optimized inventory levels.
- Faster response to disruptions and market fluctuations.
- Enhanced decision-making based on current information.
- Increased operational efficiency and reduced manual effort.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

- Map your current data flows and identify bottlenecks or manual processes, then Invest in data integration tools and systems that support real-time data processing.
- Prioritize critical data streams for real-time refresh based on their impact on decision-making to maximize the effectiveness of your data refresh initiatives.

Implementation steps

1. Identify all sources of demand and supply data within your organization and with partners.
2. Implement automated data capture and integration solutions (for example, APIs, ETL tools).
3. Establish data validation, cleansing, and governance procedures.
4. Configure real-time or near real-time data streaming for critical datasets.
5. Regularly review and optimize data refresh processes and technologies.

Operate

SCOPS10: How are operational issues managed through to resolution, ensuring corrective actions are implemented and validated?

Effective management and tracking of operational issues through resolution is vital because it minimizes disruption impact, helps prevent recurring problems, and continuously improves supply chain resilience.

SCOPS11: How is automation used to expedite the response to re-routing shipments or adjusting inventory allocations?

Using automation to expedite responses for re-routing shipments and adjusting inventory allocations is crucial because it dramatically reduces reaction time to disruptions, minimizing their impact on customer service levels and operational costs.

Best practices

- SCOPS10-BP01 Implement an orderly approach for identifying, tracking, resolving, and validating corrective actions for operational issues
- SCOPS11-BP01 Use rule-based and AI-driven automation to respond to disruptions by re-routing shipments and optimizing inventory

SCOPS10-BP01 Implement an orderly approach for identifying, tracking, resolving, and validating corrective actions for operational issues

Efficient and effective management of operational issues is paramount for continuous improvement and resilience in the supply chain. This requires establishing a centralized system for logging and tracking all operational issues, coupled with a clear process for reporting, prioritization, and assignment. Implementing a robust root cause analysis methodology for critical issues is vital to help prevent recurrence.

Developing and managing corrective and preventive action (CAPA) plans, and then diligently monitoring their implementation and effectiveness, makes sure that solutions are validated and sustained.

Furthermore, documenting lessons learned and updating standard operating procedures (SOPs) contribute to organizational learning and better knowledge management, ultimately leading to faster problem resolution, reduced downtime, and enhanced accountability.

Desired outcome: Efficient and effective resolution of operational issues, leading to continuous improvement, reduced disruptions, and enhanced supply chain performance.

Benefits of establishing this best practice:

- Faster resolution of operational problems.
- Reduced recurrence of issues through effective root cause analysis.
- Improved operational efficiency and reduced downtime.
- Enhanced accountability and ownership of issue resolution.
- Better knowledge management and organizational learning.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

- Choose an issue tracking system that is user-friendly and integrates with other supply chain systems, while training teams on root cause analysis techniques and the CAPA process. Regularly review recurring issues to identify systemic problems and implement preventive measures to avoid future occurrences.

Implementation steps

1. Establish a centralized system for logging and tracking all operational issues.
2. Define a clear process for issue reporting, prioritization, and assignment.
3. Implement a root cause analysis methodology for critical issues.
4. Develop and manage corrective and preventive action plans.
5. Monitor the implementation and effectiveness of corrective actions.
6. Document lessons learned and update standard operating procedures (SOPs).

SCOPS11-BP01 Use rule-based and AI-driven automation to respond to disruptions by re-routing shipments and optimizing inventory

To navigate the complexities of supply chain disruptions, using automation is essential for rapid and efficient responses. This involves identifying common disruption scenarios that necessitate re-routing or inventory reallocation and then implementing real-time visibility solutions for shipments and inventory. Configuring rule-based automation for frequent, less complex response actions can provide immediate benefits.

As capabilities mature, integrating optimization algorithms or AI/ML models allows for more sophisticated and dynamic adjustments. Seamless integration with transportation and warehouse management systems is crucial for execution. While automation streamlines responses, it is important to establish clear protocols for human oversight and exception handling to maintain control and address unforeseen situations. This approach ultimately leads to reduced lead times, optimized costs, improved customer satisfaction, and increased resilience in the face of unforeseen events.

Desired outcome: Rapid and efficient response to supply chain disruptions, minimizing their impact on delivery times, costs, and customer satisfaction through automated decision-making and execution.

Benefits of establishing this best practice:

- Reduced lead times and faster recovery from disruptions.
- Optimized transportation costs and inventory holding costs.
- Improved customer satisfaction through consistent delivery performance.
- Increased resilience and agility in the face of unforeseen events.
- Reduced manual effort and human error in complex decision-making.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

- Start with automating high-frequency, low-complexity re-routing or allocation scenarios while maintaining data quality and accuracy, as automation relies heavily on reliable inputs.
- Gradually introduce more sophisticated AI-driven optimization as capabilities mature and organizational readiness increases.

Implementation steps

1. Identify common disruption scenarios that require re-routing or inventory reallocation.
2. Implement real-time visibility solutions for shipments and inventory.
3. Configure rule-based automation for common response actions.
4. Integrate optimization algorithms or AI/ML models for dynamic adjustments.
5. Facilitate seamless integration with transportation and warehouse management systems.
6. Establish clear protocols for human oversight and exception handling.

Evolve

SCOPS12: How do you continuously evolve your supply chain operations?

Continuously evolving supply chain operations is essential because it enables organizations to adapt to changing market conditions, customer expectations, and technological advancements while maintaining competitive advantage.

Best practices

- SCOPS12-BP01 Establish a culture and processes for continuous improvement, innovation, and adaptation in supply chain operations

SCOPS12-BP01 Establish a culture and processes for continuous improvement, innovation, and adaptation in supply chain operations

Continuous evolution is vital for a supply chain to remain competitive and resilient. This involves establishing a formal continuous improvement program and dedicating resources to innovation initiatives. Implementing mechanisms for gathering and analyzing performance data and stakeholder feedback is crucial for identifying areas for optimization. Developing a structured process for evaluating and piloting new technologies and methodologies makes sure that the supply chain remains at the forefront of operational excellence. Fostering cross-functional teams dedicated to innovation and problem-solving, alongside investing in ongoing training and professional development for supply chain teams, creates a culture of learning and adaptation. Regularly reviewing and updating supply chain strategies based on performance insights and

market trends facilitates alignment with evolving business and customer demands, leading to enhanced efficiency, cost-effectiveness, and customer satisfaction.

Desired outcome: A highly adaptive, resilient, and continuously optimizing supply chain that consistently meets evolving business and customer demands.

Benefits of establishing this best practice:

- Increased competitive advantage through superior operational performance.
- Enhanced resilience to disruptions and market changes.
- Improved efficiency, cost-effectiveness, and customer satisfaction.
- A culture of innovation and continuous learning.
- Better alignment of supply chain with overall business strategy.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

- Dedicate resources for innovation and continuous improvement initiatives while implementing a structured process for evaluating and prioritizing improvement opportunities.
- Celebrate successes and learnings from continuous improvement efforts to reinforce the culture and encourage ongoing participation across the organization.

Implementation steps

1. Establish a formal continuous improvement program for supply chain operations.
2. Implement mechanisms for gathering and analyzing performance data and stakeholder feedback.
3. Develop a process for evaluating and piloting new AI models and methodologies.
4. Foster cross-functional teams dedicated to innovation and problem-solving.
5. Invest in ongoing training and professional development for supply chain teams.
6. Regularly review and update supply chain strategies based on performance insights and market trends.

Resources

Related documents:

- Disaster Recovery (DR) Architecture on AWS, Part IV: Multi-site Active/Active
- AWS Certificate Manager
- AWS X-Ray
- Use tags to create and maintain Amazon CloudWatch alarms for Amazon EC2 instances
- SCRM (Supply Chain Risk Management)
- SBOM (Software Bill of Materials)
- Compliance Frameworks such as NIST
- Amazon Web Services: Risk and Compliance

Security

The security pillar focuses on the ability to protect information, systems, and assets through risk assessments and mitigation strategies, while also delivering business value to the organization. Supply chain operations face unique security challenges due to their interconnected nature, involving multiple parties, systems, and jurisdictions. Organizations must navigate industry-specific requirements and various international trade regulations that evolve frequently and vary by region.

Organizations operating global supply chains must comply with different security requirements across multiple countries and regions, while managing an increasingly complex network of suppliers, partners, and service providers.

The security pillar provides an overview of design principles, best practices, and questions. You can find implementation guidance in the Security Pillar whitepaper.

Focus areas

- Design principles
- Security foundations
- Identity and access management
- Detection
- Infrastructure protection
- Data protection
- Incident response
- Application security
- Key AWS services
- Resources

Design principles

- **Identify and adhere to regulatory compliance and standards in supply chain management:** Designing high quality and adherence to regulatory compliance and standards within supply chain management is critical. AWS services provide tools and frameworks that can help customers work towards alignment with industry standards such as ISO, GDPR, and HIPAA. These tools can assist in the implementation of data integrity and security measures across the supply chain.

- **Build on secure protocols for supply chain management connectivity to the cloud:** Secure connectivity is critical for real-time data exchange in supply chain operations. MQTT is a preferred lightweight messaging protocol for its efficient data transmission, ideal for IoT applications in supply chains. Additionally, HTTPS can be employed for secure, encrypted communication between clients and the cloud. AWS IoT Core supports MQTT, and Amazon API Gateway can be configured for HTTPS.
- **Identify vulnerabilities and perform penetration testing:** Regular identification of vulnerabilities and penetration testing is essential to secure the supply chain infrastructure. This facilitates proactive risk management through regular vulnerability assessments, timely patch implementation, security updates, and systematic remediation to maintain a robust security posture and help prevent potential breaches across the entire supply chain environment.
- **Implement secure identity access management for supply chain and internal and external stakeholders:** Robust identity and access management (IAM) controls are foundational to securing the supply chain. Employing IAM roles to grant temporary access with minimized privileges, reducing the risk of unauthorized access. The use of external IDs allows secure delegation of access to AWS resources for external stakeholders, adhering to the principle of least privilege.

Security foundations

SCSEC01: How does your governance model address security and compliance requirements for your supply chain workloads?

Security and compliance requirements must be considered for supply chain workloads, a robust governance model with a Cloud Center of Excellence (CCoE) is crucial to meet security and compliance requirements.

SCSEC02: How do you maintain visibility and oversight of your supply chain security posture across multiple environments and regions?

From a supply chain perspective, maintaining compliance with regulatory guidelines and mandates is crucial for companies executing a supply chain. Traditional compliance assessment methods may

not be sufficient for the dynamic and agile cloud environment that underpins modern supply chain operations. As such, specific best practices and tools are required to facilitate compliance in the cloud-based supply chain environment. To maintain visibility and oversight of your supply chain security posture across multiple environments and regions, using cloud services for automated compliance monitoring and management is crucial.

Best practices

- SCSEC01-BP01 Establish security and governance functions in your CCoE
- SCSEC01-BP02 Use cloud services to maintain security controls while scaling your supply chain environment
- SCSEC01-BP03 Practice continuous governance
- SCSEC02-BP01 Track cloud resources and enforce compliance with automation
- SCSEC02-BP02 Aggregate findings and metrics to maintain centralized visibility

SCSEC01-BP01 Establish security and governance functions in your CCoE

A robust Cloud Center of Excellence (CCoE) should incorporate dedicated security and governance functions to implement consistent implementation of security controls across your supply chain operations. By embedding these functions within your CCoE, organizations can establish standardized security practices, compliance frameworks, and risk management processes that address the unique challenges of supply chain systems. This approach enables proactive identification and mitigation of security vulnerabilities while supporting regulatory compliance across multi-party supply chain networks. Implementing strong governance within the CCoE also facilitates clear decision-making authority, accountability structures, and continuous improvement processes for supply chain security posture.

Desired outcome: A well-structured CCoE that effectively governs cloud adoption and security practices across the organization.

Benefits of establishing this best practice: Improved security posture and compliance adherence through standardized policies and practices.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Establish a cross-functional CCoE team with representatives from security, compliance, operations, finance, and business units to drive cloud adoption and governance

The CCoE defines and enforces security policies, standards, and best practices aligned with financial industry regulations and your organization's risk posture, while treating the cloud as a product and application teams as customers to build a culture of security and compliance into everything.

Implementation steps

1. Assemble a cross-functional CCoE team with representatives from security, compliance, operations, finance, and business units, defining clear roles and establishing regular communication channels.
2. Develop comprehensive security policies and standards aligned with financial industry regulations and your organization's risk posture, including review processes for exceptions.
3. Design and implement IAM policies enforcing least privilege access and separation of duties across AWS accounts, with regular access reviews and certification processes.
4. Create self-service resources, training materials, and consultation services to build a security-first culture that treats cloud as a product and application teams as customers.
5. Deploy automated policy enforcement through guardrails, monitoring, and alerting systems to detect violations and maintain security posture visibility.
6. Establish regular governance reviews with continuous improvement cycles to adapt security practices as cloud technologies and organizational needs evolve.

SCSEC01-BP02 Use cloud services to maintain security controls while scaling your supply chain environment

Using cloud security services enables organizations to implement consistent, automated security controls that scale seamlessly with dynamic supply chain environments. These services provide built-in capabilities for threat detection, data protection, identity management, and compliance monitoring across your entire supply chain environment.

By integrating cloud security services directly into your infrastructure as code and CI/CD pipelines, you can make sure security controls are consistently applied from development through production while maintaining operational agility.

This approach reduces the operational burden on security teams while providing enhanced visibility and protection for supply chain workloads as they scale to meet changing business demands.

Desired outcome: Efficient provisioning of secure, compliance-aligned resources at scale using AWS native services.

Benefits of establishing this best practice: Streamlined governance and enhanced security through automated, consistent resource management.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

- Use cloud management and governance services like AWS Control Tower, Service Catalog, and AWS Security Hub to provision secure, compliance-aligned resources at scale.
- AWS Control Tower can help set up a secure multi-account environment following best practices for separation of duties and least privilege access, while Service Catalog allows you to create and manage pre-approved, secure IT service catalogs for your supply chain workloads.

Implementation steps

1. Deploy AWS Control Tower to establish a secure multi-account environment with guardrails that enforce separation of duties and least privilege access across your supply chain infrastructure.
2. Create standardized, pre-approved templates in Service Catalog to enable self-service provisioning of secure supply chain workloads while maintaining governance controls.
3. Implement AWS Security Hub to gain centralized visibility into security findings, automate compliance checks, and continuously monitor security best practices across supply chain accounts.
4. Use AWS Artifact to access and distribute compliance reports, certifications, and attestations that demonstrate the security posture of your cloud-based supply chain to stakeholders and auditors.
5. Configure AWS Audit Manager to automatically collect and organize evidence for regulatory compliance, simplifying audit preparation and demonstrating adherence to industry standards.
6. Integrate these services with your CI/CD pipelines and infrastructure as code to make sure security controls scale automatically with your supply chain workloads and maintain consistency across environments.

SCSEC01-BP03 Practice continuous governance

By establishing a CCoE with cross-functional collaboration, using cloud governance services, and fostering a culture of continuous improvement, your organization can effectively address security and compliance requirements for supply chain workloads in the cloud.

Desired outcome: Adaptive security policies that evolve with changing business needs and threat landscapes.

Benefits of establishing this best practice: Increased resilience to emerging threats and improved compliance through ongoing monitoring and policy updates.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Establish adaptive security policies and procedures that evolve continuously to align with dynamic business needs, system modifications, and application updates throughout the organization's lifecycle.

Continuously monitor and assess your supply chain workloads for compliance with security policies using automated tools and processes, while regularly reviewing and updating security policies and standards based on evolving threats, regulations, and business needs.

Implementation steps

1. Establish a regular cadence for reviewing and updating security policies and standards.
2. Implement automated compliance checks that run continuously across your supply chain environment.
3. Create a feedback loop between security findings and policy updates to address emerging threats.
4. Develop metrics to measure the effectiveness of security governance processes.
5. Conduct quarterly governance reviews with key stakeholders from security, operations, and business teams.
6. Document and communicate policy changes to all affected teams and partners.

SCSEC02-BP01 Track cloud resources and enforce compliance with automation

Implement automated monitoring systems to continuously track and inventory all cloud resources throughout your supply chain environment. Establish compliance guardrails with automated enforcement mechanisms that validate configurations against security and regulatory requirements before deployment.

Use automation to regularly audit existing resources, detect drift from approved configurations, and remediate non-compliant resources without manual intervention. This approach maintains consistent governance across your supply chain while reducing the operational burden of compliance management.

Desired outcome: Continuous compliance tracking and automated remediation across multiple accounts and regions.

Benefits of establishing this best practice: Real-time detection, automated fixing of non-compliant configurations, reduced risk of non-compliance and improved efficiency in managing regulatory requirements.

Level of risk exposed if this best practice is not established: high

Implementation guidance

Configure AWS Config rules to evaluate resources on a periodic or real-time basis for continuous compliance monitoring, while utilizing AWS Config and its proactive mode to automatically track and remediate resource configurations for continuous compliance across accounts and regions.

Enable AWS Security Hub standards and controls to continuously evaluate if security requirements are met across your supply chain environments, and Implement automated workflows to route security findings from AWS Security Hub to your incident response and remediation processes.

Implementation steps

1. Deploy AWS Config across the accounts and regions in your supply chain environment, configuring both periodic and change-triggered evaluation rules to monitor resource configurations against compliance standards.
2. Activate AWS Config's proactive mode to automatically remediate non-compliant resources, making sure configurations consistently meet security requirements without manual intervention.

3. Enable relevant AWS Security Hub standards (such as CIS AWS Foundations, AWS Foundational Security Best Practices, and industry-specific frameworks) to comprehensively evaluate security posture across your supply chain accounts.
4. Create custom Security Hub insights that focus specifically on supply chain-critical resources and configurations to prioritize security findings relevant to your business operations.
5. Implement automated workflows using EventBridge and Lambda to route Security Hub findings to appropriate teams, ticketing systems, and remediation processes based on severity and resource type.
6. Establish dashboards and regular reporting mechanisms that provide visibility into compliance status, trends, and remediation effectiveness across your supply chain environment.

SCSEC02-BP02 Aggregate findings and metrics to maintain centralized visibility

Centralizing security findings and metrics across your distributed supply chain environment provides comprehensive visibility into your overall security posture and enables more effective risk management. By aggregating data from multiple sources, accounts, and regions into unified dashboards, security teams can quickly identify patterns, prioritize threats, and coordinate response efforts across the entire supply chain environment.

This consolidated approach minimizes blind spots that often exist between different supply chain components and trading partners, allowing for faster detection of potential security incidents and compliance issues. Maintaining centralized visibility also supports more informed decision-making by providing executives and stakeholders with clear, actionable insights into the security health of the supply chain network.

Desired outcome: Consolidated view of compliance status across the entire supply chain infrastructure.

Benefits of establishing this best practice: Enhanced decision-making capabilities and faster response to compliance issues.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Use AWS Config's aggregated view to get a consolidated compliance picture across multiple AWS accounts and Regions, while AWS Security Hub provides a comprehensive view of your high-priority security alerts and compliance findings from across AWS accounts.

Integrate compliance data from AWS services into centralized dashboards and reporting tools for visibility into your overall supply chain security posture.

Implementation steps

1. Configure AWS Config aggregators to consolidate compliance data from all supply chain accounts and regions into a designated security account, providing a unified view of resource configurations and compliance status.
2. Enable AWS Security Hub in all accounts and establish a central administrator account to aggregate security findings, with customized security standards specific to supply chain operations.
3. Implement automated tagging strategies for all resources to categorize them by supply chain function, allowing for more granular filtering and analysis of security findings.
4. Create custom Amazon CloudWatch dashboards that integrate metrics from multiple AWS services (Config, Security Hub, Amazon GuardDuty, and Amazon Inspector) to visualize security trends and compliance status across your supply chain.
5. Develop automated reporting workflows using Amazon EventBridge, AWS Lambda, and Quick Suite to generate and distribute regular security posture summaries to stakeholders based on their roles and responsibilities.
6. Establish integration points between AWS security services and external SIEM or GRC systems to incorporate supply chain security data into enterprise-wide risk management processes.

Identity and access management

SCSEC03: How do you manage and control access to supply chain systems and data for partners, vendors, and third parties?

Managing access for partners, vendors, and third parties is critical for supply chain security as these external entities often require legitimate access to sensitive systems but represent

significant potential threat vectors if not properly controlled. Implementing robust identity management, least privilege principles, and continuous monitoring for third-party access helps prevent unauthorized data exposure and supply chain infiltration. Effective third-party access management balances operational efficiency with security requirements, enabling necessary collaboration while protecting critical supply chain assets and maintaining regulatory compliance.

SCSEC04: How do you implement least privilege access and separation of duties for supply chain operations?

Implementing least privilege access and separation of duties is fundamental to supply chain security as it minimizes the risk of unauthorized actions, fraud, and insider threats by making sure individuals have only the permissions necessary for their specific roles.

Best practices

- SCSEC03-BP01 Implement granular access controls
- SCSEC04-BP01 Implement least privilege access

SCSEC03-BP01 Implement granular access controls

Implementing granular access controls across your supply chain environment makes sure that users, systems, and third parties have precisely the level of access required for their specific functions. By defining and enforcing fine-grained permissions based on roles, responsibilities, and contextual factors such as location or time, organizations can significantly reduce the risk of unauthorized access to sensitive supply chain data and systems. This approach minimizes the potential exposure surface while maintaining operational efficiency through automated provisioning and de-provisioning processes. Regular reviews and continuous validation of access patterns help identify anomalies and maintain the principle of least privilege across complex, multi-party supply chain networks.

Desired outcome: Secure and controlled access for external parties to supply chain systems and data.

Benefits of establishing this best practice: Reduced risk of unauthorized access and improved compliance with data protection regulations.

Level of risk exposed if this best practice is not established: High

Implementation guidance

To manage and control access to supply chain systems and data for partners, vendors, and third parties, you can use various AWS services to implement robust access controls, monitoring, and governance mechanisms.

Use AWS Identity and Access Management (IAM) to create and manage federated identities, roles, and permissions for your supply chain partners and vendors, while implementing AWS IAM Identity Center to centrally manage access to multiple AWS accounts and cloud applications, including your supply chain systems.

Implementation steps

1. Implement a centralized identity management system with federation capabilities to create and manage external identities, defining granular role-based access policies that enforce least privilege principles for all third-party users and systems.
2. Deploy a single sign-on solution across your supply chain environment to streamline authentication while enforcing consistent security policies including multi-factor authentication and conditional access controls based on risk factors.
3. Establish secure private connection methods between your supply chain systems and partner environments, avoiding direct internet exposure and creating encrypted communication channels for all third-party interactions.
4. Configure comprehensive activity logging and monitoring across all supply chain systems, with automated alerts for suspicious behaviors and regular auditing of third-party access patterns and usage.
5. Implement a resource sharing framework that enables controlled access to specific supply chain resources while maintaining centralized governance and helping to prevent unauthorized lateral movement between systems.
6. Create automated onboarding and offboarding workflows for third-party access that include approval gates, time-limited access, and regular recertification processes to help prevent access sprawl and facilitate timely revocation.

SCSEC04-BP01 Implement least privilege access

Least privilege access and separation of duties create critical security boundaries between different supply chain functions, helping to prevent a single individual from controlling an entire process that could compromise data integrity or operational security.

For organizations with complex supply chains, these principles form the foundation of a zero-trust security model that protects sensitive information, maintains regulatory compliance, and preserves the integrity of supply chain operations.

Desired outcome: Minimized risk of unauthorized access and data breaches through granular access controls.

Benefits of establishing this best practice: Enhanced security posture and compliance with regulatory requirements for access control.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Define IAM policies tailored to common supply chain roles such as supplier, logistics partner, and quality inspector, and use IAM Access Analyzer to refine permissions and verify strict adherence to the principle of least privilege across your supply chain environment. Implement a multi-account strategy with dedicated Organizational Units for different supply chain functions, using service control policies to enforce restrictions on actions within these OUs, and configure custom rules to monitor and enforce supply chain-specific compliance requirements.

Implementation steps

1. Design a role-based access control framework with supply chain-specific roles, mapping each role to precisely defined permissions that align with job responsibilities and implementing automated access analyzers to identify and remove excessive permissions.
2. Implement a multi-account architecture with dedicated Organizational Units for distinct supply chain functions, using service control policies to enforce boundaries between operational areas and help prevent unauthorized actions across account boundaries.
3. Configure automated compliance monitoring with custom rules to detect violations of separation of duties, track changes to critical supply chain resources, and facilitate proper implementation of access controls across all environments.
4. Develop standardized, pre-approved resource templates for common supply chain workloads with embedded security controls and access constraints that enforce least privilege by default during provisioning.
5. Establish automated workflows for access requests, approvals, and provisioning that incorporate appropriate segregation of duties checks and maintain audit trails of all access changes across the supply chain environment.

6. Implement regular access reviews and certification processes specific to supply chain roles, with automated detection of toxic combinations of permissions that could violate separation of duties principles.

Detection

SCSEC05: How do you monitor and detect potential security threats or anomalies across your supply chain infrastructure and applications?

Continuous monitoring and threat detection are essential for supply chain security as they enable early identification of potential breaches or anomalies across your distributed infrastructure. Effective monitoring helps prevent data breaches, service disruptions, and maintains the integrity of your supply chain operations.

Best practices

- SCSEC05-BP01 Implement comprehensive monitoring and threat detection

SCSEC05-BP01 Implement comprehensive monitoring and threat detection

Implement robust monitoring systems that provide real-time visibility across all supply chain infrastructure, applications, and data flows to quickly identify anomalous activities and performance issues. Deploy advanced threat detection capabilities that use behavioral analysis and pattern recognition to identify potential security breaches before they impact operations. Establish centralized logging and alerting mechanisms that consolidate security events from diverse sources, enabling rapid investigation and response to emerging threats. This comprehensive approach facilitates continuous protection of your supply chain environment while providing the intelligence needed to adapt security controls as threats evolve.

Desired outcome: Real-time detection and response to security threats across the supply chain environment.

Benefits of establishing this best practice: Improved threat detection capabilities and reduced time to respond to security incidents.

Level of risk exposed if this best practice is not established: high

Implementation guidance

Enable AWS CloudTrail with separate trails for critical supply chain operations, configuring event selectors for tracking Amazon S3 operations on supplier data buckets, API calls to order management systems, and cross-account activities between logistics partners. Implement Amazon GuardDuty with custom threat detection for supply chain operations, monitoring for unusual patterns such as unauthorized access to supplier portals, suspicious data transfers between trading partners, or abnormal API calls to inventory systems.

Implementation steps

1. Enable dedicated monitoring trails for critical supply chain operations, configuring event selectors to track operations on supplier data storage, API calls to order management systems, and cross-account activities between logistics partners.
2. Implement threat detection services with custom detection rules specifically designed for supply chain operations, focusing on unauthorized access to supplier portals and suspicious data transfers between trading partners.
3. Deploy automated vulnerability scanning for critical supply chain workloads including EDI gateways, order processing systems, and inventory management applications.
4. Configure centralized logging with appropriate retention policies to maintain audit trails of all supply chain activities and security events for compliance and investigation purposes.
5. Establish automated alerting mechanisms with appropriate severity levels for different types of security events, making sure the right teams receive timely notifications.
6. Regularly review and update monitoring configurations and detection rules to address emerging threats and changes in supply chain infrastructure.

Infrastructure protection

SCSEC06: How do you secure and isolate the different stages of your supply chain?

Segmenting and isolating different stages of your supply chain is crucial for limiting the blast radius of potential security incidents. This approach helps prevent lateral movement of threats and

makes sure that a compromise in one area doesn't cascade throughout your entire supply chain environment.

SCSEC07: How do you protect your supply chain systems and workloads from potential vulnerabilities or misconfigurations?

Supply chain systems are prime targets for bad actors seeking to exploit vulnerabilities or misconfigurations. Proactive identification and remediation of these weaknesses is essential to maintain the security posture of your supply chain and help prevent disruptions to business operations.

Best practices

- SCSEC06-BP01 Implement network segmentation and isolation to reduce risks across supply chain phases
- SCSEC07-BP01 Regularly scan for vulnerabilities, patch your workloads and audit your systems for compliance

SCSEC06-BP01 Implement network segmentation and isolation to reduce risks across supply chain phases

Network segmentation creates security boundaries between different stages of your supply chain, limiting the potential impact of security breaches. By implementing logical separation between procurement, manufacturing, distribution, and other supply chain functions, organizations can help prevent lateral movement of threats and apply specific security controls appropriate to each segment. This approach enables more granular access control, improved monitoring, and enhanced protection of sensitive assets across the supply chain environment. Effective segmentation should be based on business functions, data sensitivity, and regulatory requirements.

Desired outcome: Segmented and secure supply chain stages with appropriate access controls and monitoring.

Benefits of establishing this best practice: Reduced risk of cross-stage contamination and improved overall supply chain security.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Isolate procurement systems within dedicated network segments and implement least privilege access controls for procurement staff, while making sure all sensitive procurement data is encrypted both at rest and in transit. Isolate manufacturing systems into separate network zones with stringent access control lists, and establish secure private connectivity channels between manufacturing processes and supply chain partners.

Implementation steps

1. Isolate procurement systems within dedicated network segments and implement least privilege access controls for procurement staff, while making sure all sensitive procurement data is encrypted both at rest and in transit.
2. Separate manufacturing systems into separate network zones with stringent access control lists, and establish secure private connectivity channels between manufacturing processes and supply chain partners.
3. Deploy web application protection to shield distribution applications from common web-based exploits and vulnerabilities.
4. Implement comprehensive monitoring and threat detection across all distribution systems to identify unauthorized access attempts and behavioral anomalies.
5. Establish consistent security tagging and classification schemes across all supply chain stages to enable automated security policy enforcement and compliance verification.
6. Regularly conduct security assessments and penetration testing for each supply chain stage to identify and remediate vulnerabilities before they can be exploited.

SCSEC07-BP01 Regularly scan for vulnerabilities, patch your workloads and audit your systems for compliance

Maintaining a proactive vulnerability management program is critical for identifying and addressing security weaknesses across supply chain systems. This involves implementing regular scanning processes to detect vulnerabilities in infrastructure, applications, and dependencies used throughout the supply chain. Establishing systematic patching procedures makes sure that identified vulnerabilities are remediated in a timely manner based on risk assessment and business impact. Complementing these activities with regular compliance audits helps verify that security controls are functioning as intended and meeting regulatory requirements.

Desired outcome: Proactive identification and remediation of vulnerabilities across supply chain systems.

Benefits of establishing this best practice: Reduced threat surface and improved resilience against potential security threats.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Implement automated vulnerability scanning to continuously assess supply chain-specific workloads, configuring custom assessment templates for EDI gateways, supplier portals, and order management systems to prioritize patching based on supply chain impact and criticality metrics.

Deploy automated patch management to maintain security across supply chain applications, creating patch baselines specific to different workload types and coordinating patch deployments with trading partners to minimize supply chain disruptions.

Implementation steps

1. Implement automated vulnerability scanning to continuously assess supply chain-specific workloads, configuring custom assessment templates for EDI gateways, supplier portals, and order management systems to prioritize patching based on supply chain impact and criticality metrics.
2. Deploy automated patch management to maintain security across supply chain applications, creating patch baselines specific to different workload types and coordinating patch deployments with trading partners to minimize supply chain disruptions.
3. Enable continuous compliance monitoring with custom controls aligned with supply chain frameworks, tracking configuration changes to maintain compliance with industry standards across your supply chain infrastructure.
4. Establish a centralized security dashboard to provide visibility into vulnerability status, patch compliance, and security posture across all supply chain components and partner integrations.
5. Implement automated remediation workflows that trigger corrective actions when critical vulnerabilities or compliance violations are detected in supply chain systems.
6. Create regular reporting mechanisms to communicate security status to stakeholders and document compliance with regulatory requirements specific to supply chain operations.

Data protection

SCSEC08: How do you manage and protect encryption keys used within your supply chain systems?

Encryption keys are critical security assets that protect sensitive supply chain data both at rest and in transit. Proper key management supports data confidentiality and integrity across your supply chain network, while helping to prevent unauthorized access to protected information.

SCSEC09: How do you classify and handle sensitive supply chain data (for example, product designs, pricing, and logistics)?

Supply chains process various types of sensitive data that require different levels of protection. Proper classification and handling of this data is essential to apply appropriate security controls, meet compliance requirements, and help prevent competitive disadvantages from data breaches.

SCSEC10: How are you encrypting supply chain data at rest and in transit across different environments?

Encryption is a fundamental security control for protecting supply chain data as it moves through various systems and networks. Implementing comprehensive encryption strategies safeguards sensitive information from unauthorized access and helps maintain compliance with industry regulations.

Best practices

- SCSEC08-BP01 Implement strong key management in your supply chain systems
- SCSEC09-BP01 Implement data classification and protection
- SCSEC10-BP01 Implement comprehensive data encryption

SCSEC08-BP01 Implement strong key management in your supply chain systems

Effective encryption key management is fundamental to protecting sensitive data across supply chain operations. This includes implementing secure processes for key generation, storage, rotation, and revocation throughout the key lifecycle. Organizations should establish clear separation of duties for key management activities and make sure keys are protected with strong access controls. Regular auditing of key usage and implementing automated rotation schedules helps maintain the integrity of encryption throughout the supply chain environment.

Desired outcome: Secure and controlled management of encryption keys throughout the supply chain systems, supporting data protection and compliance.

Benefits of establishing this best practice: Enhanced data security, reduced risk of unauthorized access, and improved compliance through centralized key management.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Manage encryption keys across different supply chain stages, creating separate keys for distinct operations (supplier data, logistics documents, customs documentation) with rotation policies aligned to compliance requirements. Implement key policies and access controls that reflect supply chain partner relationships, using temporary access grants during specific supply chain events like customs inspections or quality audits.

Implementation steps

1. Manage encryption keys across different supply chain stages, creating separate keys for distinct operations (supplier data, logistics documents, customs documentation) with rotation policies aligned to compliance requirements.
2. Implement key policies and access controls that reflect supply chain partner relationships, using temporary access grants during specific supply chain events like customs inspections or quality audits.
3. Enable comprehensive key usage monitoring focused on supply chain-critical operations, tracking encryption activities across trade documentation, cross-border data transfers, and partner data exchanges.
4. Configure automated alerts for unusual encryption key usage patterns that might indicate supply chain process violations or security incidents.

5. Establish a centralized encryption governance framework that documents key ownership, usage purposes, and access patterns across the entire supply chain environment.
6. Create regular key inventory and access review processes to make sure encryption controls remain aligned with evolving supply chain relationships and compliance requirements.

SCSEC09-BP01 Implement data classification and protection

A comprehensive data classification framework enables organizations to identify and appropriately protect different types of supply chain information. This approach involves categorizing data based on sensitivity, regulatory requirements, and business impact to apply proportionate security controls. Organizations should implement automated discovery and classification tools to identify sensitive data across diverse supply chain systems. Protection mechanisms should align with classification levels, making sure that the most sensitive information receives the strongest safeguards while maintaining operational efficiency.

Desired outcome: Accurate classification and appropriate protection of sensitive supply chain data.

Benefits of establishing this best practice: Improved data protection and compliance with data privacy regulations.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Implement automated data classification using machine learning and discovery tools to identify and categorize sensitive supply chain data such as product designs, pricing information, and logistics data. Apply encryption for sensitive data at rest across all storage services, facilitating consistent protection of supply chain information regardless of where it resides.

Implementation steps

1. Implement automated data classification using machine learning and discovery tools to identify and categorize sensitive supply chain data such as product designs, pricing information, and logistics data.
2. Apply encryption for sensitive data at rest across all storage services, facilitating consistent protection of supply chain information regardless of where it resides.
3. Define granular access control policies that enforce least privilege principles for accessing and managing sensitive supply chain data across all systems and user roles.

4. Manage digital certificates centrally to facilitate secure encrypted data transmission between supply chain systems, partners, and service providers.
5. Establish data handling procedures that automatically apply appropriate controls based on data classification, including retention policies, access restrictions, and encryption requirements.
6. Implement regular data protection audits to verify classification accuracy and control effectiveness, adjusting rules and policies as supply chain data sensitivity evolves.

SCSEC10-BP01 Implement comprehensive data encryption

A holistic encryption strategy is essential for protecting supply chain data throughout its lifecycle. This includes implementing strong encryption for data at rest in storage systems, databases, and backup media across all supply chain environments. Complementary transport encryption should secure data as it moves between systems, partners, and geographic locations. Organizations should select appropriate encryption algorithms and key lengths based on data sensitivity and regulatory requirements, while making sure that encryption implementation doesn't significantly impact system performance or user experience.

Desired outcome: Comprehensive encryption of supply chain data throughout its lifecycle.

Benefits of establishing this best practice: Enhanced data protection and reduced risk of data breaches or unauthorized access.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Implement a centralized encryption key management strategy with regular key rotation schedules to protect supply chain data across all services and integrate with broader encryption features. Configure server-side encryption for all object storage containing supply chain data using appropriate key management options based on sensitivity levels and compliance requirements.

Implementation steps

1. Implement a centralized encryption key management strategy with regular key rotation schedules to protect supply chain data across all services and integrate with broader encryption features.
2. Configure server-side encryption for all object storage containing supply chain data using appropriate key management options based on sensitivity levels and compliance requirements.

3. Enable encryption for all relational database instances that store supply chain information, selecting the appropriate key management approach based on security requirements and operational needs.
4. Activate encryption for all block storage volumes supporting supply chain applications to facilitate data protection at the storage layer regardless of application-level encryption.
5. Establish an encryption governance framework that documents which encryption methods are applied to different types of supply chain data and systems based on classification and risk assessment.
6. Implement automated compliance monitoring to verify that encryption controls remain consistently applied as supply chain infrastructure evolves and new resources are provisioned.

Incident response

SCSEC11: How do you prepare for and respond to potential security incidents impacting your supply chain operations?

Security incidents in supply chain environments can have far-reaching consequences, disrupting operations and affecting multiple stakeholders. A well-defined incident response strategy enables rapid containment, minimizes operational impact, and facilitates swift recovery from security breaches.

SCSEC12: How do you enable traceability and forensic analysis of security events across the supply chain?

Comprehensive logging and forensic capabilities are essential for investigating security incidents across complex supply chain environments. Effective traceability allows organizations to understand the scope of incidents, identify root causes, and implement appropriate remediation measures.

Best practices

- SCSEC11-BP01 Develop and implement a comprehensive incident response plan
- SCSEC12-BP01 implement comprehensive logging and forensic analysis framework

SCSEC11-BP01 Develop and implement a comprehensive incident response plan

Establish a comprehensive incident response plan tailored specifically for supply chain disruptions that clearly defines roles, responsibilities, and escalation procedures across all stakeholders including suppliers and logistics partners. Regularly conduct tabletop exercises and simulations to test the effectiveness of response protocols under various supply chain threat scenarios, making sure teams are prepared to act decisively during actual incidents.

Implement automated detection mechanisms that can quickly identify potential supply chain security breaches or operational disruptions, triggering appropriate response workflows. Maintain secure communication channels and documentation procedures that enable effective coordination during incidents while preserving evidence for post-incident analysis and continuous improvement of security controls.

Desired outcome: A comprehensive and well-tested incident response plan tailored for supply chain operations.

Benefits of establishing this best practice: Faster response times to security incidents and minimized impact on supply chain operations.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Maintain an up to date incident response plan specifically for supply chain incidents, with defined roles, communication procedures, and playbooks that are regularly reviewed and tested through tabletop exercises. Use AWS Security Hub to aggregate security alerts and compliance checks across AWS accounts and supply chain partners' connected accounts, providing a centralized view of security posture.

Implementation steps

1. Develop a comprehensive incident response plan specifically tailored for supply chain operations, including defined roles, responsibilities, and escalation procedures for all stakeholders.
2. Implement centralized security monitoring and alerting systems to aggregate findings from multiple sources and provide unified visibility into supply chain security posture.

3. Establish automated incident detection and response workflows that can quickly identify and respond to supply chain-specific security threats and operational disruptions.
4. Configure comprehensive logging and monitoring across all supply chain infrastructure to enable forensic analysis and incident investigation capabilities.
5. Create secure backup and recovery procedures for critical supply chain data and systems, with immutable backups stored in separate secured environments.
6. Conduct regular tabletop exercises and incident response simulations to test and refine response procedures, making sure all teams are prepared for various supply chain threat scenarios.

SCSEC12-BP01 implement comprehensive logging and forensic analysis framework

Implement a robust logging and monitoring framework that captures detailed audit trails across all supply chain systems, applications, and partner interactions to enable thorough forensic analysis of security events. Deploy centralized log management solutions that aggregate and correlate security data from diverse sources, providing investigators with comprehensive visibility into supply chain activities and potential security incidents. Establish automated analysis capabilities that can quickly process large volumes of log data to identify patterns, anomalies, and indicators of compromise across the extended supply chain network. Maintain appropriate log retention policies and secure storage mechanisms to make sure forensic evidence remains available and tamper-proof for compliance and investigation purposes.

Desired outcome: Comprehensive logging and monitoring framework for efficient forensic analysis of security events.

Benefits of establishing this best practice: Improved ability to investigate and resolve security incidents, enhancing overall supply chain security.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Implement comprehensive logging from all supply chain systems and applications into centralized log management solutions, providing a single source of truth for security and operational data. Use AWS CloudTrail to record API activity across AWS accounts in the supply chain environment, enabling detailed auditing of actions and changes across the infrastructure.

Implementation steps

1. Centralize logging from all supply chain systems and applications into a unified log management solution that provides comprehensive visibility and search capabilities.
2. Configure detailed API activity logging across all AWS accounts and services used in the supply chain environment to maintain complete audit trails.
3. Implement automated log analysis and correlation capabilities to rapidly identify security incidents and anomalous activities across the supply chain network.
4. Deploy specialized forensic analysis tools that can visualize and analyze security data to identify root causes and impact of security incidents.
5. Establish appropriate log retention policies and secure storage mechanisms to make sure forensic evidence remains available for compliance and investigation requirements.
6. Create automated reporting and alerting mechanisms that notify security teams of potential incidents and provide initial analysis to accelerate response efforts.

Application security

SCSEC13: How do you incorporate security practices within the software development lifecycle for supply chain applications?

Integrating security throughout the software development lifecycle is crucial for building secure supply chain applications from the ground up. This approach helps identify and address vulnerabilities early, reducing the cost and impact of security issues in production environments.

SCSEC14: How do you validate the integrity of supply chain application code and dependencies?

Supply chain applications rely on numerous code dependencies that can introduce security vulnerabilities if not properly validated. Maintaining the integrity of application code and dependencies helps prevent supply chain attacks and maintains the trustworthiness of your systems.

Best practices

- SCSEC13-BP01 Integrate security throughout the software development lifecycle
- SCSEC14-BP01 Implement comprehensive code and dependency integrity validation

SCSEC13-BP01 Integrate security throughout the software development lifecycle

Incorporate security measures into the earliest stages of the software development lifecycle (SDLC) to support robust protection throughout the development process. Develop policies and procedures for secure coding practices where developers are trained to follow industry-standard guidelines. Implement security requirements during the requirements phase, design secure architectures during the design phase, develop secure code during implementation, conduct thorough security testing, and maintain secure deployment and maintenance practices. This comprehensive approach makes sure that security is not an afterthought but an integral part of the development process for supply chain applications.

Desired outcome: Security integrated throughout the SDLC, resulting in more secure supply chain applications.

Benefits of establishing this best practice: Reduced vulnerabilities in supply chain applications and lower costs associated with fixing security issues post-deployment.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Integrate security measures into the earliest stages of the Software Development Life Cycle (SDLC) to support robust protection throughout the development process. Develop policies and procedures for secure coding practices, where developers are trained to follow industry-standard guidelines for supply chain-specific requirements including product identification and tracking, secure data exchange protocols for supplier communications, and trade partnership security requirements for cross-border operations.

Implementation steps

1. Define security standards and requirements specific to supply chain operations during the requirements phase, including product identification, tracking, and secure data exchange protocols.

2. Design secure architectures during the design phase that implement chain of custody patterns, secure B2B integration patterns, and data isolation models for multi-party supply chain networks.
3. Develop secure APIs and Implement digital signature frameworks during the implementation phase, focusing on real-time inventory tracking, shipment monitoring, and electronic proof of delivery.
4. Conduct comprehensive security testing including penetration testing specific to B2B integration points, security audits on business message flows, and compliance testing with industry-specific regulations.
5. Implement secure deployment practices including key management for cross-organizational data sharing, continuous monitoring for supply chain-specific threat patterns, and incident response procedures for supply chain disruptions.
6. Establish ongoing security maintenance practices including regular security assessments, vulnerability management, and security training for development teams working on supply chain applications.

SCSEC14-BP01 Implement comprehensive code and dependency integrity validation

Maintaining the integrity of application code and dependencies is critical for helping to prevent supply chain attacks that target software components. Organizations should implement code signing to verify authenticity and help prevent tampering with application components. Automated scanning of dependencies for known vulnerabilities should be integrated into development workflows to identify security issues before deployment. Establishing trusted repositories for approved components and implementing integrity verification during build and deployment processes creates multiple layers of protection against compromised software in the supply chain.

Desired outcome: Verified and secure code and dependencies throughout the supply chain application lifecycle.

Benefits of establishing this best practice: Reduced risk of compromised applications and improved overall security of the supply chain environment.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Use code signing to verify the authenticity and integrity of code, involving digitally signing the code with a cryptographic key to validate it has not been tampered with. Use tools like AWS CodeArtifact to manage and securely store dependencies, making sure only approved and verified dependencies are used in applications, while regularly scanning dependencies for known vulnerabilities using automated security scanning tools.

Implementation steps

1. Implement code signing processes to digitally sign all application code and components, supporting authenticity and helping to prevent tampering throughout the development and deployment lifecycle.
2. Establish secure dependency management using trusted repositories and automated scanning tools to identify and remediate vulnerabilities in third-party components before deployment.
3. Implement strict access controls and audit logs in source control systems to track changes and make sure only authorized personnel can modify code and dependencies.
4. Integrate automated security checks into CI/CD pipelines to validate code and dependency integrity during build and deployment processes, helping to prevent compromised components from reaching production.
5. Deploy runtime protection measures and monitoring tools to detect and respond to unauthorized changes or suspicious activities in real-time during application execution.
6. Establish comprehensive monitoring and logging systems to maintain visibility into code and dependency integrity across the entire application lifecycle and supply chain environment.

Key AWS services

The AWS service that is essential to security is AWS Identity and Access Management, which allows you to securely control access to AWS services and resources for your users. The following services and features support the four areas of security:

Identity and access management:

- AWS Identity and Access Management: Control users' access to and usage of AWS. Create and manage users and groups and grant or deny access. Implement strong authorization and authentication.

- AWS IAM Identity Center: Centrally manage workforce access to multiple AWS accounts and applications
- AWS Directory Service: Set up and run directories in AWS or connect your AWS resources with an existing Active Directory.
- Amazon Cognito: Implement secure, frictionless customer identity and access management that scales.

Detection:

- Amazon CloudWatch Logs: Observe and monitor resources and applications on AWS, on-premises, and on other clouds.
- Amazon Detective: Investigate and analyze potential security issues or suspicious activities in their AWS environments.
- Amazon GuardDuty: Protect your AWS accounts with intelligent threat detection.
- Amazon Inspector: Automated and continual vulnerability management at scale.
- AWS CloudTrail: Track user activity and API usage.
- AWS Config: Assess, audit, and evaluate configurations of your resources.
- AWS Security Hub: Automate AWS security checks and centralize security alerts.

Infrastructure protection:

- AWS Key Management Service: Create and control keys used to encrypt or digitally sign your data
- AWS WAF: Protect your web applications from common exploits

Data protection:

- Amazon Macie: Discover and protect your sensitive data at scale
- Amazon CloudFront: Distribute web content, including dynamic, static, streaming, and interactive content, to users
- Application Load Balancer: Distribute incoming application traffic across multiple targets, such as EC2 instances, containers, and IP addresses
- AWS Config: Assess, audit, and evaluate configurations of your resources
- AWS Systems Firewall: Deploy network firewall security across your VPCs

- AWS Virtual Private Network: Define and launch AWS resources in a logically isolated virtual network

Incident response:

- AWS Lambda: Run code without thinking about servers or clusters
- AWS Audit Manager Continuously audit your AWS usage to simplify how you assess risk and compliance with regulations and industry standards.
- AWS Compliance Center: Research cloud-related regulatory requirements

Resources

- AWS Shield Advanced capabilities and options
- AWS Digital Sovereignty Pledge: Control without compromise
- Security, Identity, and Compliance on AWS
- Amazon Web Services: Risk and Compliance
- AWS Clean Rooms
- Why AWS Data Exchange?

Reliability

The reliability pillar includes recommendations for a supply chain workload to perform its intended function correctly and consistently. This includes the ability to operate and test the workload through its total lifecycle. This paper provides in-depth, best practice guidance for implementing reliable supply chain workloads on AWS.

The reliability pillar provides an overview of design principles, best practices, and questions. You can find implementation guidance in the Reliability Pillar whitepaper.

Focus areas

- Design principles
- Foundation
- Change management
- Failure management
- Key AWS services
- Resources

Design principles

- **Inventory and order data synchronization:** Design systems to provide continuous synchronization of inventory and order data across warehouses, distribution centers, and online storefronts to help prevent stockouts or overselling.
- **Implement supplier and logistics redundancy:** Architect supply chain solutions with backup suppliers and logistics providers, facilitating seamless transitions during disruptions.
- **Enable demand-driven scalability:** Build systems that can scale inventory allocation, procurement, and transportation dynamically based on real-time demand forecasts.
- **Design for transportation route resilience:** Incorporate alternate routing options and real-time transportation updates to mitigate risks such as traffic delays, weather conditions, or geopolitical disruptions.
- **Integrate real-time shipment and delivery tracking:** Use IoT devices and logistics tracking APIs to monitor the location and condition of goods, facilitating timely interventions for delays or damage.

- **Automate disruption recovery for supply chain processes:** Use predictive models and automation to reroute shipments, reallocate inventory, or switch suppliers quickly during failures or unexpected events.

Foundation

SCREL01: How do you establish redundancy for key suppliers and logistics providers?

Single points of failure in suppliers or logistics providers can disrupt the entire supply chain, leading to missed delivery timelines or unfulfilled orders.

SCREL02: How do you maintain holistic visibility of shipments and deliveries?

Holistic visibility makes sure that stakeholders can track the location, status, and condition of goods, enabling timely interventions for delays or issues.

Best practices

- SCREL01-BP01 Identify suppliers and logistics partners and establish backup agreements or alternate sourcing strategies to mitigate risks
- SCREL02-BP01 Integrate shipment tracking solutions, providing real-time visibility through IoT devices and logistics APIs

SCREL01-BP01 Identify suppliers and logistics partners and establish backup agreements or alternate sourcing strategies to mitigate risks

Identifying critical suppliers and logistics partners is essential for building supply chain resilience, as these relationships often represent single points of failure that can severely impact operations when disrupted. Organizations should conduct thorough risk assessments to categorize partners based on their operational importance, substitutability, and geographic concentration. For high-risk dependencies, establish formal backup agreements with alternative providers who can quickly activate during disruptions, while maintaining appropriate inventory buffers for critical components. Implement regular testing of these contingency arrangements through simulated

disruption scenarios to validate their effectiveness and refine response protocols before real emergencies occur.

Desired outcome: A resilient supply chain that can seamlessly transition to alternate suppliers or carriers during disruptions.

Benefits of establishing this best practice: Minimizes the impact of supplier failures, geopolitical issues, or natural disasters on supply chain operations.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Building redundancy into supplier and logistics partnerships makes sure the supply chain remains resilient during disruptions. Use AWS Supply Chain to analyze and identify dependencies on critical suppliers and logistics providers, while automated procurement systems can be configured to switch to alternative suppliers when needed. Maintaining real-time communication through APIs with logistics providers allows for prompt responses to operational issues.

Implementation steps

1. **Analyze dependencies**: Use AWS Supply Chain to identify critical supplier and logistics dependencies.
2. **Establish backup agreements**: Create agreements with alternate suppliers and logistics providers.
3. **Automate supplier switching**: Implement automated procurement systems for seamless supplier transitions.
4. **Real-time communication**: Use APIs for real-time communication with logistics providers.

SCREL02-BP01 Integrate shipment tracking solutions, providing real-time visibility through IoT devices and logistics APIs

Integrate comprehensive shipment tracking solutions with core supply chain systems to create end-to-end visibility across transportation networks, warehouses, and last-mile delivery operations. Deploy IoT devices such as GPS trackers, temperature sensors, and shock monitors to capture real-time condition and location data from shipments, while establishing API connections with logistics partners to incorporate their tracking information into a unified visibility system. Implement

geofencing capabilities to automatically trigger notifications and workflow actions when shipments enter or exit predefined geographic boundaries, enabling proactive exception management.

This enhanced visibility infrastructure provides stakeholders with accurate estimated arrival times, condition monitoring, and chain-of-custody verification, significantly improving customer experience while reducing operational uncertainty.

Desired outcome: A fully transparent supply chain where all stakeholders have real-time access to shipment information, enhancing accountability and responsiveness.

Benefits of establishing this best practice: Improves customer satisfaction, reduces operational inefficiencies, and enables better decision-making in case of delays.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

End-to-end visibility requires integrating IoT devices and logistics APIs into the supply chain. AWS IoT FleetWise can be used to gather vehicle and shipment data, while dashboards created with Quick Suite provide stakeholders with real-time insights. Providing customers with tracking links further enhances transparency.

Implementation steps

1. **Deploy IoT tracking devices**: Use AWS IoT FleetWise for collecting shipment data.
2. **Create visualization dashboards**: Use Quick Suite to display real-time shipment data.
3. **Provide customer tracking**: Share real-time tracking links with customers for enhanced transparency.
4. **Monitor visibility systems**: Regularly assess the visibility tools for accuracy and efficiency.

Change management

SCREL03: How do you dynamically adjust transportation routes based on real-time condition s?

Transportation delays caused by traffic, weather, or other disruptions can significantly impact delivery timelines and customer satisfaction.

Best practices

- SCREL03-BP01 Integrate route optimization tools with real-time data from logistics providers and IoT sensors to dynamically adjust routes

SCREL03-BP01 Integrate route optimization tools with real-time data from logistics providers and IoT sensors to dynamically adjust routes

Implement advanced route optimization tools that continuously recalculate optimal delivery paths by incorporating real-time data streams from traffic systems, weather services, and vehicle telematics. Connect these optimization engines with IoT sensors deployed across the logistics network to capture immediate feedback on road conditions, vehicle performance, and cargo status, enabling dynamic rerouting decisions when disruptions occur. Establish bidirectional integration with logistics partners' systems to synchronize schedule changes, resource availability, and delivery constraints across the extended transportation network. This intelligent routing environment should support multi-objective optimization that balances competing priorities like fuel efficiency, delivery time windows, driver hours-of-service constraints, and carbon emissions targets while adapting to changing conditions throughout the execution cycle.

Desired outcome: A transportation network capable of rerouting shipments to minimize delays and allow on-time delivery.

Benefits of establishing this best practice: Reduces delivery lead times, avoids penalties for late deliveries, and improves overall supply chain efficiency.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Dynamic route adjustment relies on integrating route optimization tools with real-time data. Services such as AWS IoT Core provides real-time location tracking, while Amazon Location Service can help optimize routes based on current conditions. Collaborate with logistics providers that offer dynamic routing capabilities to enable rerouting decisions that are efficiently executed.

Implementation steps

1. **Deploy real-time tracking**: Use AWS IoT Core to track shipment locations.
2. **Integrate route optimization tools**: Use Amazon Location Service for dynamic route planning.

3. **Collaborate with logistics providers**: Partner with providers offering advanced routing capabilities.
4. **Monitor rerouting efficiency**: Regularly evaluate and improve the effectiveness of routing adjustments.

Failure management

SCREL04: How do you synchronize inventory and order data in real-time across all nodes in the supply chain?

Real-time synchronization enables inventory availability, procurement decisions, and customer orders are based on accurate and up-to-date information. This helps prevent issues like overselling, unfulfilled orders, or inventory wastage.

SCREL05: How do you monitor and mitigate the risks of product spoilage or damage during transit?

Certain goods, such as perishable food or sensitive electronics, require strict environmental conditions during transit to maintain quality and usability.

SCREL06: How do you use predictive analytics to anticipate supply chain disruptions?

Predicting potential disruptions, such as demand surges, supplier delays, or geopolitical risks, enables proactive planning to avoid operational bottlenecks.

Best practices

- SCREL04-BP01 Implement a centralized inventory and order management system integrated with all warehouses, suppliers, and sales channels
- SCREL05-BP01 Deploy IoT-based monitoring systems to track temperature, humidity, and other environmental factors during transit

- SCREL06-BP01 Use machine learning models to analyze historical data and external factors, predicting disruptions and optimizing inventory

SCREL04-BP01 Implement a centralized inventory and order management system integrated with all warehouses, suppliers, and sales channels

Use event-driven architectures to propagate updates across the supply chain. Implement a centralized inventory and order management system that provides a single source of truth for product availability, allocations, and fulfillment status across all physical and digital channels. Establish real-time integration with warehouse management systems, supplier portals, and sales systems to synchronize inventory movements and order status changes throughout the fulfillment lifecycle.

Deploy event-driven architecture patterns that take immediate actions when significant changes occur, such as automatically reallocating inventory when stock levels reach thresholds or initiating replenishment workflows when demand signals change. This interconnected system should support sophisticated allocation rules that optimize inventory placement based on factors like customer promise dates, fulfillment costs, and service level agreements while maintaining data consistency across all supply chain nodes.

Desired outcome: An integrated supply chain system where inventory levels and order statuses are consistent and accurate across all nodes.

Benefits of establishing this best practice: Helps prevent customer dissatisfaction caused by overselling or delays and reduces excess inventory costs by maintaining accurate stock levels.

Level of risk exposed if this best practice is not established: High

Implementation guidance

To enable real-time synchronization of inventory and order data, adopt an event-driven architecture that propagates updates seamlessly across the supply chain. Tools like AWS EventBridge or Amazon Managed Streaming for Apache Kafka (Amazon MSK) can handle real-time event streaming to enable data sharing across all nodes immediately. Data integration from various sources, such as warehouses and sales channels, should utilize services like AWS Glue or Amazon AppFlow. Regular audits of synchronization logs will help identify and address inconsistencies promptly, safeguarding the accuracy of supply chain data.

Implementation steps

1. **Set up event-driven architecture**: Configure AWS EventBridge or Apache Kafka to manage real-time data streaming for inventory and order updates.
2. **Integrate data nodes**: Use AWS Glue or Amazon AppFlow to connect data sources like warehouses, suppliers, and online storefronts.
3. **Audit data regularly**: Implement scheduled audits of synchronization logs to help with data consistency across all nodes.
4. **Monitor system performance**: Deploy monitoring tools to track the efficiency of data synchronization and resolve issues as they arise.

SCREL05-BP01 Deploy IoT-based monitoring systems to track temperature, humidity, and other environmental factors during transit

Deploy comprehensive IoT-based monitoring systems throughout your supply chain to continuously track critical environmental conditions like temperature, humidity, shock, light exposure, and location for sensitive products during storage and transit. Configure these systems with product-specific thresholds that trigger immediate alerts when measurements deviate from acceptable ranges, enabling rapid intervention before product quality is compromised.

Implement a centralized monitoring dashboard that visualizes real-time condition data across all shipments, with drill-down capabilities to investigate anomalies and historical trend analysis to identify recurring issues. These monitoring capabilities should integrate with quality management systems to automatically document compliance with regulatory requirements and customer specifications while providing complete chain-of-custody verification for sensitive or high-value products.

Desired outcome: A supply chain where environmental conditions are actively monitored and controlled to improve product quality.

Benefits of establishing this best practice: Reduces losses due to spoilage or damage, increases customer satisfaction, and compliance with regulatory requirements.

Level of risk exposed if this best practice is not established: High

Implementation guidance

To mitigate risks of spoilage or damage, deploy IoT sensors to monitor environmental conditions such as temperature and humidity. Use AWS IoT SiteWise to analyze this data in real-time and implement automated alerts to detect deviations. Regular testing of IoT sensors improves reliability, enabling proactive management of risks during transit.

Implementation steps

1. **Install IoT sensors**: Deploy sensors to monitor critical environmental conditions during transit.
2. **Analyze data in real-time**: Use AWS IoT SiteWise to collect and analyze sensor data.
3. **Set up alerts**: Implement automated alerts for deviations in environmental conditions.
4. **Test and maintain sensors**: Regularly test sensors to enable accuracy and reliability.

SCREL06-BP01 Use machine learning models to analyze historical data and external factors, predicting disruptions and optimizing inventory

Implement machine learning models that analyze patterns across historical supply chain disruptions, correlating them with external factors such as weather events, geopolitical developments, and economic indicators to identify emerging risk patterns. Train predictive algorithms on comprehensive datasets that combine internal operational metrics with external variables to forecast potential disruption impacts on specific supply chain nodes and transportation lanes.

Deploy these predictive insights through automated decision support systems that recommend preemptive inventory positioning, transportation mode shifts, and supplier diversification strategies before disruptions materialize. Continuously refine these models through feedback loops that compare predicted outcomes with actual events, enabling progressive improvement in disruption forecasting accuracy and response optimization over time.

Desired outcome: A proactive supply chain that adapts to potential risks before they occur, minimizing disruptions and maintaining service levels.

Benefits of establishing this best practice: Improves operational agility, reduces response times, and enhances supply chain resilience.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Predictive analytics involves using machine learning models to anticipate supply chain disruptions. Use Amazon Forecast for demand prediction and Amazon SageMaker AI to develop custom models for disruption prediction. Continuously updating and training these models with the latest data facilitates ongoing accuracy and effectiveness.

Implementation steps

1. **Implement predictive models**: Use Amazon Forecast and Amazon SageMaker AI for predictive analytics.
2. **Analyze historical data**: Integrate historical and external data to train the models.
3. **Update models continuously**: Retrain models with updated data to improve predictions.
4. **Develop mitigation strategies**: Use predictions to plan inventory and logistics adjustments proactively.

Key AWS services

- Amazon EventBridge: A serverless event bus that connects applications using events from your applications, SaaS providers, or AWS services, offering real-time data synchronization.
- AWS Glue: A serverless data integration service that simplifies data preparation, loading, and ETL (Extract, Transform, Load) processes.
- Amazon AppFlow: A service for automating data transfers between AWS services and SaaS applications without code.
- AWS Supply Chain: A specialized service for managing and analyzing supply chain dependencies, enabling redundancy and automated supplier transitions.
- AWS IoT Core: A service for connecting IoT devices to the cloud, enabling real-time monitoring and data collection from devices like shipment trackers.
- Amazon Location Service: Provides APIs for map rendering, geocoding, and routing, used for real-time route optimization and planning.
- AWS IoT SiteWise: A managed service for collecting, storing, and analyzing IoT data, particularly useful for monitoring environmental factors like temperature and humidity during transit.
- Amazon Forecast: A machine learning service for building accurate forecasts using time-series data.

- Amazon SageMaker AI: A machine learning service for building, training, and deploying models at scale, used for disruption prediction and optimization.
- AWS IoT FleetWise: Enables collection and transmission of data from vehicles and shipments to the cloud for analysis.
- Quick Suite: A business intelligence service for creating interactive dashboards to visualize shipment and supply chain data.
- AWS Lambda: A serverless compute service that runs code in response to events, such as updates in data streams or file uploads, enabling real-time processing for supply chain events.
- Amazon S3: A scalable object storage service used for storing supply chain data, logs, and backups securely and efficiently.

- Amazon CloudWatch: A monitoring service that provides data and actionable insights to verify application performance and operational health. It can monitor supply chain systems, log synchronization events, and trigger alarms when anomalies occur.

Resources

Related documents:

- AWS Supply Chain
- What is AWS Supply Chain?
- Mitigating operational risks with AWS Supply Chain Work Order Insights
- Addressing industry-specific supply chain challenges with AWS Supply Chain
- AWS Supply Chain Workshop

Related videos:

- AWS Supply Chain Resources

Performance efficiency

The performance efficiency pillar encompasses the ability to optimize supply chain operations and resources to meet business requirements while maintaining efficiency as market demands fluctuate and supply chain technologies advance. Key topics include selecting appropriate logistics solutions and capacity planning based on supply chain requirements, monitoring operational performance through KPIs, and making data-driven decisions to enhance throughput and reduce bottlenecks. Whether managing warehouse operations, transportation networks, or inventory systems, performance efficiency makes sure that supply chain resources are utilized effectively to deliver maximum value.

For more information, see Performance Efficiency Pillar - AWS Well-Architected Framework.

Focus areas

- Design principles
- Architecture selection
- Compute selection
- Database and storage selection
- Network architecture selection
- Test and monitor performance
- Key AWS services
- Resources

Design principles

Select your architecture based on performance data. Evaluate metrics across all architectural components, including system design patterns, resource type performance, and configuration benchmarks. Review architectural decisions quarterly to use new AWS Cloud capabilities. Monitor specific performance indicators against established baselines and implement corrections when metrics fall outside defined thresholds. Optimize performance through targeted techniques such as data compression, strategic caching, and balanced consistency models.

Following are the key design principles for performance efficiency for supply chain:

- **Use managed services and purpose-built applications:** AWS provides several managed services like databases, compute, and storage and purpose-built application for business like AWS Supply Chain, which can assist your architecture in increasing the overall reliability, performance, security and quicker onboarding of workloads.
- **Democratize advanced technologies:** Make advanced technology implementation easier for your team by delegating complex tasks to the cloud. Rather than asking your IT team to learn about hosting and running a new technology, consider consuming the technology as a service. For example, NoSQL databases, media transcoding, and AI/ML are all technologies that require specialized expertise. In the cloud, these technologies become services that your team can consume, allowing your team to focus on product development rather than resource provisioning and management.
- **Use serverless architectures:** Serverless architectures remove the need for you to run and maintain physical servers for traditional compute activities. For example, serverless storage services can act as static websites (removing the need for web servers) and event services can host code. This removes the operational burden of managing physical servers and can lower transactional costs because managed services operate at cloud scale.
- **Experiment more often:** With virtual and automated resources, you can quickly carry out comparative testing using different types of instances, storage or configurations.

Architecture selection

SCPERF01: How do you select the best performing architecture?

Performance objectives for workloads can vary depending on the criticality of the workload. While more stringent performance requirements are expected for critical supply chain systems, such as global supply and demand, sourcing and procurement, and inbound and outbound logistics, cloud workloads still benefit from defining performance requirements.

Best practices

- SCPERF01-BP01 Use internal and external risk to determine performance requirements
- SCPERF01-BP02 Factor in rate of increase in load, traffic, and scale-out intervals

SCPERF01-BP01 Use internal and external risk to determine performance requirements

External regulatory or supplier systems, as well as internal risk requirements, are often a good place to start for performance requirements. For certain systems, regulators release sector-wide guidance and data residency rules and regulators require that system have the capability to deliver on the operational resilience and the performance targets they have set for themselves.

Desired outcome: You can achieve best end-user performance irrespective of the data residency rules due to the regulatory requirements.

Benefits of establishing this best practice: Low latency, best end-user experience, and low risk of violating data regulations.

Level of risk exposed if this best practice is not established: High

Implementation guidance

External regulatory or supplier systems, as well as internal risk requirements, are often a good place to start for performance requirements. For certain systems, regulators release sector-wide guidance and data residency rules and regulators require that system have the capability to deliver on the operational resilience and the performance targets they have set for themselves. If the systems update the supplier database or connected to their network to pull data, the performance targets should be taken into consideration.

Implementation steps

1. Identify all relevant regulatory requirements and data residency rules that apply to your supply chain systems.
2. Analyze supplier system performance requirements and integration points that may impact overall system performance.
3. Establish performance baselines based on regulatory guidance and internal risk assessments.
4. Define performance targets that balance compliance requirements with operational efficiency.
5. Implement monitoring and alerting systems to track performance against established targets.
6. Regularly review and update performance requirements as regulations and business needs evolve.

SCPERF01-BP02 Factor in rate of increase in load, traffic, and scale-out intervals

Identify the upper bounds of the peak load against a system, as well as the amount of time needed to reach peak load. Load tests often overlook the rate of increase in traffic and create tests that scale up too quickly or too slowly.

Desired outcome: You mimic the traffic and load situation of the system and see how the user experience in such situations, this will help to fine-tune the underlying resources of the architecture to achieve better results.

Benefits of establishing this best practice: System resiliency prediction, and system behavior during peak hours/loads.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Identify the upper bounds of the peak load against a system, as well as the amount of time needed to reach peak load. Load tests often overlook the rate of increase in traffic and create tests that scale up too quickly or too slowly. If the load test ramps up too quickly, the system may not be able to add capacity rapidly enough to meet the demand, which degrades performance and introduces errors. Load tests need to be run periodically and with every major release of the system or when new systems or architecture is introduced in the supply chain eco-system.

Implementation steps

1. Analyze historical traffic patterns to identify peak load periods and growth rates specific to supply chain operations.
2. Design load tests that accurately simulate realistic traffic ramp-up patterns based on actual usage scenarios.
3. Establish automated scaling policies that can respond appropriately to gradual and sudden load increases.
4. Implement comprehensive monitoring during load tests to identify performance bottlenecks and capacity constraints.
5. Create regular load testing schedules that coincide with major system releases and supply chain system integrations.

6. Document and analyze load test results to continuously improve system performance and scaling capabilities.

Compute selection

SCPERF02: How do you select your compute architecture?

The optimal compute solution for a particular architecture depends on the workload deployment method, degree of automation, usage patterns, and configuration. Third-party solutions in a supply chain environment like transport management system (TMS), order management system (OMS), and customer management systems (CRMs) can bring their own requirements for infrastructure, which must also be considered.

Best practices

- SCPERF02-BP01 Use serverless compute to run tasks
- SCPERF02-BP02 Use machine learning capabilities for supply chain applications
- SCPERF02-BP03 Use edge compute capabilities for supply chain applications

SCPERF02-BP01 Use serverless compute to run tasks

Choosing the correct compute power for the workload provides smooth performance of the application, not only for the end users also for the solution developer community to maintain the software stacks across various infrastructures.

Desired outcome: Smooth performance that elastic in nature with low upkeep.

Benefits of establishing this best practice: Improved user experience, maintenance of software stack, and scalability.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Some supply chain services computing workloads, like supplier data visibility, are typically loosely coupled and can benefit from event-driven architectures using the scaling capacity of AWS

serverless compute options like AWS Lambda and AWS Fargate, combined with messaging services including Amazon SQS and Amazon EventBridge to decouple components. These serverless solutions minimize the overhead of capacity management, automatically scaling in or out to meet demands. Where scale is the primary factor, AWS serverless container compute engine AWS Fargate, can be used with both Amazon Elastic Container Service (Amazon ECS) and Amazon Elastic Kubernetes Service (Amazon EKS), removing the overhead of managing and provisioning compute resources.

Implementation steps

1. Identify supply chain workloads that are suitable for serverless architectures, focusing on event-driven and loosely coupled processes.
2. Implement AWS Lambda functions for lightweight, short-duration tasks such as data processing and API integrations.
3. Deploy AWS Fargate for containerized workloads that require more control over the runtime environment while maintaining serverless benefits.
4. Integrate messaging services like Amazon SQS and Amazon EventBridge to decouple components and enable asynchronous processing.
5. Configure auto-scaling policies to automatically adjust compute resources based on demand patterns and workload requirements.
6. Monitor performance metrics and optimize function configurations to facilitate efficient resource utilization and cost-effectiveness.

SCPERF02-BP02 Use machine learning capabilities for supply chain applications

AWS Supply Chain unifies data and provides machine learning--powered actionable insights, built-in contextual collaboration, and demand planning.

Desired outcome: High requirement workloads can be made easier using machine learning capabilities. Certain pre-built algorithms can reused to fit your workflow which can save time for building the right solutions.

Benefits of establishing this best practice: Agility, performance, and re-usability.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Use AWS Supply Chain to reduce the heavy lifting of the workloads, which involves deep machine learning skills and time-consuming algorithm development activities.

Implementation steps

1. Evaluate existing supply chain processes to identify opportunities where machine learning can provide value and improve efficiency.
2. Implement AWS Supply Chain to use pre-built machine learning models for demand forecasting and supply planning.
3. Integrate machine learning capabilities with existing supply chain systems to enhance decision-making and automation.
4. Train teams on machine learning tools and best practices to maximize the value of AI-powered supply chain solutions.
5. Monitor machine learning model performance and continuously refine algorithms based on actual business outcomes.
6. Expand machine learning usage to additional supply chain use cases as capabilities and confidence grow.

SCPERF02-BP03 Use edge compute capabilities for supply chain applications

AWS offers a robust suite of edge computing solutions that extend cloud capabilities closer to end users, devices, and on-premises locations. At the core of AWS's edge computing strategy are two main services: AWS Outposts and AWS Local Zones.

Desired outcome: These edge compute capabilities enable a single-digit millisecond latency for applications like supply chain which needs real-time edge data to perform machine learning inferences and action autonomously without pushing the decision making at the cloud.

Benefits of establishing this best practice: Agility, performance, and low latency.

Level of risk exposed if this best practice is not established: High

Implementation guidance

AWS offers a robust suite of edge computing solutions that extend cloud capabilities closer to end users, devices, and on-premises locations. At the core of AWS's edge computing strategy are two main services: AWS Outposts and AWS Local Zones. AWS Outposts brings native AWS services, infrastructure, and operating models to virtually any datacenter or on-premises facility. It's ideal for workloads requiring low latency access to on-premises systems, local data processing, or data residency requirements. AWS Local Zones are infrastructure deployments that place compute, storage, database, and other AWS services closer to large population and industry centers. Local Zones act as an extension of an AWS Region, connected through high-bandwidth, secure connections.

Implementation steps

1. Assess supply chain operations to identify use cases that require low-latency processing or local data residency.
2. Deploy AWS Outposts for on-premises workloads that need AWS services with local data processing capabilities.
3. Implement AWS Local Zones for applications requiring ultra-low latency access to end users or manufacturing facilities.
4. Configure AWS IoT Greengrass for edge devices to enable local data processing and autonomous decision-making capabilities.
5. Establish secure connectivity between edge locations and central cloud infrastructure to maintain data synchronization.
6. Monitor edge computing performance and optimize resource allocation to facilitate efficient operation across distributed locations.

Database and storage selection

SCPERF03: How do you select the database and storage for supply chain workloads?

When you select a database or storage solution, verify that it aligns with your access patterns to achieve the desired performance. AWS has predefined set of purpose-built databases engines

(Relational or Non-relational) which suits for different data that the source system produces, and such systems can scale for performance.

Best practices

- SCPERF03-BP01 Select your database architecture based on workload
- SCPERF03-BP02 Select your storage architecture based on workload
- SCPERF03-BP03 Use cache memory to help improve the performance

SCPERF03-BP01 Select your database architecture based on workload

Purpose-built data storage for your workloads can help increase the performance efficiency of the overall system, as well to be more resilient in case of failures.

Desired outcome: Purpose-built data storage. Increased performance efficiency of the overall system.

Benefits of establishing this best practice: Scalability, resilience, and end user performance improvement.

Level of risk exposed if this best practice is not established: High.

Implementation guidance

Select database options that align with your performance requirements, using different database technologies for different purposes, such as Amazon Timestream time-series database for storing ticking market data, rather than a one-size-fits-all use of traditional relational databases. Also, Amazon RDS is a straightforward relational database service optimized for total cost of ownership. It is simple to set up, operate, and scale with demand. Amazon RDS automates the undifferentiated database management tasks, such as provisioning, configuring, backups, and patching.

Implementation steps

1. Analyze supply chain data access patterns and performance requirements to determine optimal database architectures.
2. Implement purpose-built databases for specific use cases, such as time-series databases for IoT sensor data and document databases for product catalogs.
3. Configure Amazon RDS for transactional supply chain data that requires ACID compliance and complex queries.

4. Deploy NoSQL databases like Amazon DynamoDB for high-throughput, low-latency applications such as inventory tracking.
5. Establish database performance monitoring and optimization processes to maintain continued efficiency as data volumes grow.
6. Implement automated backup and disaster recovery strategies to maintain data availability and business continuity.

SCPERF03-BP02 Select your storage architecture based on workload

Data lineage is important in the world of producers and consumers of the data. This lineage can be verified and validated when it is tracked from the source system to the destination systems. As a result, well-organized data leads to better understanding.

Desired outcome: Well-organized data with improved understanding.

Benefits of establishing this best practice: Data lineage, scalability, resilience, and re-usability.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

AWS Supply Chian needs a data lake with AI/ML models for supply chains to understand, extract, and transform disparate, incompatible data into a unified data model. The data lake can ingest your data from various data sources, including your existing ERP systems, such as SAP S/4HANA, and supply chain management systems. To add data from variable sources such as EDI 856, some applications use AI/ML and natural language processing (NLP) to associate data from source systems to the unified data model. EDI 850 and 860 messages are transformed directly with predefined but customizable transformation recipes.

Implementation steps

1. Design a data lake architecture using Amazon S3 to store diverse supply chain data from multiple sources and formats.
2. Implement data ingestion pipelines using AWS Glue to extract, transform, and load data from ERP systems and supply chain applications.
3. Configure AI/ML models to process and standardize disparate data formats, including EDI messages and unstructured documents.

4. Establish data lineage tracking mechanisms to maintain visibility into data flow from source systems to destination applications.
5. Implement data governance policies and access controls to maintain data quality and security across the storage architecture.
6. Create automated data validation and quality monitoring processes to maintain data integrity throughout the supply chain environment.

SCPERF03-BP03 Use cache memory to help improve the performance

Cache memory provides improved latency of the application when accessed outside of the solution-hosted Regions.

Desired outcome: Low latency of the application when accessed outside of designated Regions.

Benefits of establishing this best practice: Better throughput, low latency, reduced power consumption, improved reliability, and increased scalability.

Level of risk exposed if this best practice is not established: High

Implementation guidance

While considering using the cache memory for your supply chain solutions, you can architect the solution to use caching services to improve performance. Store frequently used data in memory or bring the data closer to consumers. Many AWS services offer features for caching or dedicated services including Amazon ElastiCache, and Amazon File Cache. For example, frequently accessed inventory data should be stored in cache memory, with time-to-live (TTL) settings configured to align with the data's update frequency and usage patterns. In this case, data caching solutions (Redis Cache or MemoryDB) are important to quickly access last available data with low latency (200 milliseconds or less) interval.

Implementation steps

1. Identify frequently accessed supply chain data that would benefit from caching, such as inventory levels, product information, and pricing data.
2. Implement Amazon ElastiCache with Redis or Memcached to cache frequently accessed data and reduce database load.
3. Configure appropriate TTL settings for cached data based on update frequency and business requirements for data freshness.

4. Deploy Amazon CloudFront for caching static content and API responses to improve global access performance.
5. Implement cache invalidation strategies to maintain data consistency when underlying data changes.
6. Monitor cache performance metrics and optimize cache configurations to maximize hit rates and minimize latency.

Network architecture selection

SCPERF04: How do you select your network architecture for supply chain application?

Proximity to data sources, both internal and external, and the distance between components can be a key factor for supply chain workloads, like high-frequency supplier networking and manufacturing systems from factory floors, so make use of AWS services to sit your solution as close as possible to dependencies.

Best practices

- SCPERF04-BP01 Use performance requirements to drive the selection of network components and architecture

SCPERF04-BP01 Use performance requirements to drive the selection of network components and architecture

Bring the hosted solution closer to your users' Region to provide a better user experience and make the data safer while hosted or in transit.

Desired outcome: Better user experience and safer data while at rest or in transit.

Benefits of establishing this best practice: Secured data while hosted or in-transit, and low latency by using Amazon backbone network and infrastructure.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Use AWS Direct Connect to provide the shortest and most reliable path to AWS resources for components hosted outside of AWS. Use Amazon CloudFront to cache static content closer to use cases, and AWS Global Accelerator to route connections to the closest possible source, using the AWS backbone network and bringing your solutions closer to industries, users, and data. When using multiple AWS Regions, use Route 53 latency-based routing to serve requests from the AWS Region with the lowest latency.

Implementation steps

1. Analyze network performance requirements and identify optimal AWS regions based on user and supplier locations.
2. Implement AWS Direct Connect for dedicated, high-bandwidth connections between on-premises supply chain systems and AWS.
3. Deploy Amazon CloudFront to cache frequently accessed content and reduce latency for global supply chain users.
4. Configure AWS Global Accelerator to optimize network paths and improve application performance for distributed supply chain operations.
5. Implement Route 53 latency-based routing to automatically direct traffic to the best-performing AWS region.
6. Monitor network performance metrics and optimize routing configurations to maintain optimal user experience.

Test and monitor performance

SCPERF05: How do you test and monitor the performance of the supply chain systems?

Performance monitoring and testing are critical components of supply chain management as they make sure systems can handle varying loads, maintain reliability during peak operations, and provide visibility into system behavior across complex, interconnected supply chain networks. Without proper monitoring and testing, organizations risk service disruptions, poor customer experiences, and inability to identify performance bottlenecks before they impact business operations.

Best practices

- SCPERF05-BP01 Implement comprehensive monitoring and dashboards for supply chain performance
- SCPERF05-BP02 Evaluate compliance with performance requirements
- SCPERF05-BP03 Integrate performance testing into the release cycle of the supply chain application

SCPERF05-BP01 Implement comprehensive monitoring and dashboards for supply chain performance

Building an effective dashboard involves focusing on the key performance indicators (KPIs) that matter most to your organization and displaying them in an understandable and visually appealing way.

Desired outcome: Measuring of the application behavior can help manage it better, just not only the performance of the application also during vulnerable situations and to take actions spontaneously.

Benefits of establishing this best practice: Good observability and dashboard to monitor performance efficiency and continuous improvements.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Use tools and best practices to gain insights including End-to-end visibility, alerts and alarms, Anomaly detection, regular review of metrics and logs, security monitoring, and cost optimization. Remember, while AWS provides observability tools (Amazon CloudWatch, AWS CloudTrail) to monitor and gain insights, it's the combination of these tools with best practices that will give you the most valuable insights about the end-to-end supply chain systems.

Implementation steps

1. Identify key performance indicators (KPIs) that are most critical to supply chain operations and business objectives.
2. Design and implement comprehensive dashboards using Quick Suite or CloudWatch dashboards to visualize supply chain performance.

3. Configure automated alerts and alarms based on performance thresholds and anomaly detection to enable proactive response.
4. Implement end-to-end tracing and monitoring across all supply chain components, from edge devices to cloud applications.
5. Establish regular review processes for performance metrics and logs to identify trends and optimization opportunities.
6. Create role-based dashboard views that provide relevant insights to different stakeholders across the supply chain organization.

SCPERF05-BP02 Evaluate compliance with performance requirements

When many systems, including third-party systems, are involved in a workload, it is important to know the behavior of each system and to monitor who is contributing to performance loss so proper adjustments can be made.

Desired outcome: Optimum performance that conforms to the system requirements to handle loads.

Benefits of establishing this best practice: Enhanced visibility into system performance across complex supply chain networks, improved ability to identify and resolve performance bottlenecks, better accountability for third-party system performance, and reduced mean time to resolution for performance issues.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Monitoring of your workload at multiple levels helps verify that your resources are performing as expected and you are aware of deviations. Consider all dimensions of the solution for monitoring, for example client-side and server-side metrics, application metrics and infrastructure metrics, technical and functional metrics.

Provide visibility of data loss in your metrics, for example, by monitoring for lost messages.

Where possible capture inter-solution and inter-process communication streams to aid with the reproduction of issues.

Implementation steps

1. Establish performance baselines and SLAs for all supply chain systems, including third-party integrations.
2. Implement comprehensive monitoring across all system layers, including infrastructure, application, and business metrics.
3. Deploy distributed tracing to track performance across complex supply chain workflows and identify bottlenecks.
4. Create automated performance testing and validation processes to make sure systems meet established requirements.
5. Implement alerting mechanisms that notify teams when performance deviates from established baselines or SLA thresholds.
6. Conduct regular performance reviews and optimization initiatives based on monitoring data and compliance assessments.

SCPERF05-BP03 Integrate performance testing into the release cycle of the supply chain application

Load testing results help you measure how the system behaves while in high-traffic or heavy loads. Note these measurements to help you adjust the underlying resources without wasting cost by over-provisioning.

Desired outcome: Properly sized supply chain applications.

Benefits of establishing this best practice: Cost optimization, resilience, durability, and improved user experience.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Verify consistency and failure recovery during load tests. Verify data consistency and recovery during periods of high load. Making sure that your workload's RTO and RPO is still valid under the highest load can uncover gaps in your architecture and operational resilience.

Understand performance of the system under peak load and in failure scenarios: Include testing of common failure scenarios in your performance testing suites to understand your workload behavior in these situations and determine areas for improvement.

Implementation steps

1. Develop comprehensive performance testing strategies that simulate realistic supply chain load patterns and peak usage scenarios.
2. Integrate automated performance testing into CI/CD pipelines to validate performance with every major release.
3. Implement chaos engineering practices to test system resilience and recovery capabilities under various failure conditions.
4. Create performance test scenarios that include third-party system integrations and supplier network dependencies.
5. Establish performance regression testing to make sure new releases don't degrade existing system performance.
6. Document and analyze performance test results to continuously improve system architecture and resource allocation strategies.

Key AWS services

- AWS Supply Chain
- Amazon SageMaker AI
- AWS CloudWatch
- Amazon EC2
- AWS Compute Optimizer
- AWS Client VPN
- AWS Direct Connect
- Amazon Connect
- Amazon S3
- Amazon Simple Notification Service (SNS)
- Amazon RDS

Resources

Related documents:

- Addressing industry-specific supply chain challenges with AWS Supply Chain
- Mitigating operational risks with AWS Supply Chain Work Order Insights
- A prescriptive approach for AWS Supply Chain proof of values (PoVs)
- Enhancing supply chain agility with AWS Supply Chain Vendor Lead Time Insights

Related partner solutions:

- AWS Supply Chain Partners
- AWS Supply Chain Competency Partners
- Browse Solutions for supply chain

Related workshops:

- AWS Supply Chain Workshop

Related videos:

- AWS Supply Chain Resources

Cost optimization

The cost optimization pillar provides guidance on managing resources efficiently and aligning supply chain costs with business objectives. It focuses on optimizing resource utilization across materials, transportation, and warehousing while balancing speed-to-market requirements. By implementing strategic cost management practices, organizations can maximize the economic benefits of cloud-based deployments while maintaining competitive advantage in supply chain operations.

Focus areas

Design principles

In addition to the general Well-Architected cost optimization design principles, there are some design principles specific for cost optimization for supply chain. These principles encompass the key aspects of cost optimization in the supply chain domain while using AWS services and capabilities. They focus on aligning costs with value, optimizing data management, automating operations, and maintaining ongoing cost optimization efforts.

- **Align cost with supply chain value and scalability:** In supply chain, activity-based costing is crucial. Controlling costs on an activity level requires visibility, transparency and large-scale reporting. Explainability of each costing item is an industry requirement. Accurately calculating each costing item necessitates comprehensive supply chain visibility, emphasizing the need for transparency, data integration, and collaboration with suppliers and logistics partners.
- **Optimize data management and processing:** Emphasize data efficiency and relevance in supply chain operations. Choose cost-effective and efficient locations for data processing. Implement secure and cost-effective data storage solutions.

- **Automate and streamline operations:** Design for automation and efficiency to reduce manual tasks and minimize errors. Use services like AWS Lambda and AWS Step Functions for workflow automation. Implement cost-effective architectures that enhance supply chain responsiveness and efficiency. Introducing Robotics, computer vision and tracking systems reduce long term costs and increases efficiency and accuracy.
- **Continuously monitor and optimize costs:** Use AWS Cost Management tools to monitor, analyze, and optimize spending to foster a culture of cost awareness across teams. Regularly review AWS usage and costs to identify savings opportunities. Implement lifecycle policies for data management and cost-efficient resource utilization.

Align cost with value and scalability

SCCOST01: How do you balance your scalability requirements against overall IT infrastructure cost considerations?

Balancing scalability requirements against IT infrastructure costs is essential for supply chain operations because it makes sure that systems can handle demand fluctuations while maintaining cost efficiency and operational effectiveness.

Best practices

- SCCOST01-BP01 Optimize integration and collaboration across the supply chain management
- SCCOST01-BP02 Adopt a flexible and scalable cloud infrastructure

SCCOST01-BP01 Optimize integration and collaboration across the supply chain management

Supply chain optimization, enhanced by location intelligence, can minimize unnecessary miles, resulting in a cost-effective approach to logistics and transportation management.

Desired outcome: An integrated and optimized supply chain system with real-time and accurate inventory or location.

Benefits of establishing this best practice: Reduced cost and better customer satisfaction.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Capture real-time tracking events to orchestrate and streamline operations and provide visibility to your customers, while deploying cloud-based integration systems to automate and streamline communication with suppliers, transporters, and service providers. This significantly reduces manual data entry and processing tasks, leading to improved operational efficiency and cost reduction.

Implementation steps

1. Implement real-time tracking systems to capture and process supply chain events as they occur.
2. Deploy cloud-based integration systems to automate communication with suppliers, transporters, and service providers.
3. Establish automated data synchronization processes to reduce manual data entry and processing tasks.
4. Create unified dashboards that provide real-time visibility into supply chain operations for all stakeholders.
5. Implement location intelligence solutions to optimize routing and reduce unnecessary transportation costs.
6. Monitor integration performance and continuously optimize processes to maximize cost savings and operational efficiency.

SCCOST01-BP02 Adopt a flexible and scalable cloud infrastructure

A typical supply chain landscape will include ERPs, warehouse management systems (WMS), and transportation management systems (TMS) running on a large infrastructure that needs to be reliable, scalable and optimized for cost and performance.

Desired outcome: Pay as you go cloud infrastructure configured with auto scaling to expand or shrink as per demand of the workload. Cloud service quotas configured for peak usage.

Benefits of establishing this best practice: Reduced cost and better resiliency.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Use AWS' pay-as-you-go model to align costs with actual usage and demand fluctuations, while implementing auto scaling capabilities to automatically adjust resources based on workload

demands. Configure service quotas to accommodate peak usage for respective services and use containerization and serverless technologies for improved resource utilization and cost optimization.

Implementation steps

1. Assess current infrastructure costs and identify opportunities for pay-as-you-go optimization.
2. Implement auto-scaling policies for compute, storage, and database resources based on demand patterns.
3. Configure appropriate service quotas to handle peak usage while avoiding unnecessary over-provisioning.
4. Deploy containerization technologies to improve resource utilization and reduce infrastructure costs.
5. Implement serverless architectures for event-driven workloads to minimize idle resource costs.
6. Establish cost monitoring and alerting mechanisms to track spending and identify optimization opportunities.

Optimize data management and processing

SCCOST02: How do you optimize compute and data storage within supply chain systems?

In supply chain, data storage includes data such as customer and supplier data, services, and product catalogues. It also includes transactional data around orders, shipments, and tracking events. Supply chain data management is a critical driver of innovation and efficiency, offering valuable insights but requiring skillful handling of its volume, velocity, and variety to maximize value and minimize costs.

Best practices

- SCCOST02-BP01 Have a plan for your raw data storage to optimize cost
- SCCOST02-BP02 Query and retrieve data by partitions to save cost and improve performance
- SCCOST02-BP03 Only store useful data and discard the rest

SCCOST02-BP01 Have a plan for your raw data storage to optimize cost

Effective data management strategies can substantially lower expenses related to maintaining vast data volumes. Object storage is recommended for large-scale unstructured data due to its robustness, nearly unlimited capacity, scalability, and advanced metadata capabilities.

Desired outcome: A well-defined data storage strategy for the vast amount of structured or unstructured data generated by SCM systems which is cost-efficient and aligned with business requirements.

Benefits of establishing this best practice: Reduced cost, optimized performance, and improved customer satisfaction.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Implement object storage with appropriate storage classes to manage voluminous supply chain data efficiently, using Amazon S3 Standard for frequently accessed data, Amazon Glacier for archiving, and S3 Intelligent-Tiering for dynamic allocation based on usage patterns.

Employ schema-on-read services like Amazon Athena to query data in its original format, reducing storage costs, and implement data lifecycle policies to automate transitions between storage classes.

Implementation steps

1. Analyze data access patterns and classify supply chain data based on frequency of access and business criticality.
2. Implement appropriate Amazon S3 storage classes for different data types, optimizing costs based on access patterns.
3. Configure S3 Intelligent-Tiering for data with changing or unknown access patterns to automatically optimize storage costs.
4. Deploy Amazon Athena for cost-effective querying of data in its original format without requiring data transformation.
5. Establish automated data lifecycle policies to transition data between storage classes and archive or delete obsolete data.
6. Monitor storage costs and usage patterns regularly to identify additional optimization opportunities.

SCCOST02-BP02 Query and retrieve data by partitions to save cost and improve performance

Optimize data access by using partitioned queries to enhance cost-efficiency and performance in supply chain systems.

Desired outcome: Data access requirements are taken into consideration while defining data storage strategy.

Benefits of establishing this best practice: Reduced cost, optimized performance, and better customer satisfaction

Level of risk exposed if this best practice is not established: High

Implementation guidance

Organize supply chain data by time, geography, or other relevant criteria to enhance storage efficiency and reduce retrieval costs.

Implement data partitioning strategies to divide large volumes into manageable chunks based on specific characteristics like time or product ID, focusing query operations on relevant segments and reducing scanned data volume and associated costs.

Implementation steps

1. Analyze supply chain data access patterns to identify optimal partitioning strategies based on time, geography, or product categories.
2. Implement data partitioning in storage systems to organize data into logical segments that align with query patterns.
3. Configure query engines to use partition pruning to scan only relevant data segments during retrieval operations.
4. Use AWS Glue for automated data partitioning and Amazon S3's integrated compression options to further reduce costs.
5. Implement partition management processes to maintain optimal partition sizes and help prevent partition proliferation.
6. Monitor query performance and costs to continuously optimize partitioning strategies and data organization.

SCCOST02-BP03 Only store useful data and discard the rest

A well-designed supply chain data management architecture incorporates a data lake to store processed and normalized useful data, while raw data is either discarded or archived in cost-effective storage for potential future needs.

Desired outcome: Data lifecycle is well defined as per business and regulatory requirements.

Benefits of establishing this best practice: Reduced cost, optimized performance, and better customer satisfaction

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Implement data sanitization to identify, clean, and validate critical information before cloud transfer, while pre-processing data to improve bandwidth efficiency, reduce storage costs, and support high-quality, secure cloud data.

Use edge computing for local analytics and decision-making, prioritizing critical data for immediate cloud transmission.

Implementation steps

1. Establish data classification and retention policies that define what data should be kept, archived, or discarded based on business and regulatory requirements.
2. Implement automated data sanitization processes to clean and validate data before storage, removing unnecessary or redundant information.
3. Deploy edge computing solutions for local data processing and filtering, transmitting only essential data to the cloud.
4. Configure automated data lifecycle management to archive or delete data according to established retention policies.
5. Implement data quality monitoring to make sure only valuable, accurate data is retained in storage systems.
6. Regularly review and optimize data retention policies based on changing business needs and regulatory requirements.

Automate and streamline operations

SCCOST03: How do you optimize your network consumption and interactions between plant floor and overall IT infrastructure?

Optimizing network consumption and payload size is crucial for efficient data communication between industrial plants and the cloud, especially with limited bandwidth and real-time processing needs.

Best practices

- SCCOST03-BP01 Compress and aggregate data whenever possible to reduce the amount of data that needs to be transmitted over the network
- SCCOST03-BP02 Adjust collection frequency depending on the context
- SCCOST03-BP03 Choose the right communication service and configuration depending on the use case

SCCOST03-BP01 Compress and aggregate data whenever possible to reduce the amount of data that needs to be transmitted over the network

Maximizing processing and sanitation of data reduces the amount of data to be sent and processed in the cloud, leading to significant cost savings and improved performance.

Desired outcome: A well-defined strategy on where data gets processed and transmitted to reduce unnecessary load on the network and cloud

Benefits of establishing this best practice: Reduced cost, optimized performance, and better customer satisfaction

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Maximize processing and sanitation of the data in-situ, to reduce the amount of data to be sent and processed in the cloud. AWS IoT Greengrass v2 can help with processing and summarization

of data at the edge, while implementing data filtering and aggregation at the edge using AWS IoT Core rules engine or AWS IoT Greengrass v2 components to send only relevant, summarized data to the cloud.

Implementation steps

1. Identify data processing opportunities at the edge to reduce the volume of data transmitted to the cloud.
2. Deploy AWS IoT Greengrass v2 for local data processing, filtering, and aggregation at manufacturing facilities.
3. Implement data compression techniques and Combine multiple measurements into single messages to reduce transmission costs.
4. Configure AWS IoT Core rules engine to filter and route only relevant data to cloud storage and processing systems.
5. Establish data summarization processes that aggregate detailed operational data into meaningful insights before cloud transmission.
6. Monitor network usage and data transmission costs to continuously optimize edge processing strategies.

SCCOST03-BP02 Adjust collection frequency depending on the context

Optimize data collection frequency based on business needs and context using event-based triggers and thresholds to reduce costs while maintaining performance and efficiency.

Desired outcome: A well-defined collection strategy which meets the business and functional requirements.

Benefits of establishing this best practice: Reduced cost, optimized performance, and better customer satisfaction

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Optimize data collection frequency based on functional and business needs to minimize unnecessary transmission and improve efficiency in supply chain systems.

Implement event-based or context-dependent collection schemes using tools like AWS IoT Greengrass components to dynamically adapt data gathering, while defining threshold values and triggers for specific events or parameters to determine when to adjust collection frequency.

Implementation steps

1. Analyze business requirements to determine optimal data collection frequencies for different types of supply chain data.
2. Implement event-based data collection that triggers only when significant changes or thresholds are reached.
3. Configure dynamic collection frequency adjustment based on operational context and business priorities.
4. Deploy AWS IoT Greengrass components to enable intelligent, context-aware data collection at edge locations.
5. Establish threshold-based triggers that automatically adjust collection frequency based on operational conditions.
6. Monitor data collection costs and effectiveness to continuously optimize collection strategies.

SCCOST03-BP03 Choose the right communication service and configuration depending on the use case

Tailor your communication service selection and setup to match specific supply chain scenarios and requirements.

Desired outcome: A well-defined formatting/transmission strategy which meets the functional requirements of downstream applications and the entire SCM environment.

Benefits of establishing this best practice: Reduced cost, optimized performance, and better customer satisfaction

Level of risk exposed if this best practice is not established: High

Implementation guidance

Use AWS B2B Data Interchange to automatically convert Electronic Data Interchange (EDI) documents into JSON and XML formats, while utilizing MQTT 5 protocol for lightweight communication between sensors and AWS IoT Core. Implement AWS IoT Core device shadow to

store and synchronize device states, reducing the need for constant communication, and employ caching mechanisms to store frequently accessed data locally.

Implementation steps

1. Assess communication requirements for different supply chain use cases and select appropriate protocols and services.
2. Implement AWS B2B Data Interchange for efficient EDI document processing and format conversion.
3. Deploy MQTT 5 protocol for lightweight, efficient communication between IoT devices and cloud services.
4. Configure AWS IoT Core device shadow for state synchronization and reduced communication overhead.
5. Implement local caching mechanisms to minimize cloud requests and reduce bandwidth consumption.
6. Optimize Quality of Service (QoS) levels and routing paths to balance reliability with cost efficiency.

Continuously monitor and optimize costs

SCCOST04: How do you regularly analyze and fine-tune supply chain overall IT infrastructure expenses for peak efficiency?

Regular analysis and fine-tuning of supply chain IT infrastructure expenses is essential for maintaining cost efficiency while achieving optimal performance and meeting evolving business requirements.

Best practices

- SCCOST04-BP01 Use AWS services and advanced analytics to optimize overall supply chain costs
- SCCOST04-BP02 Implement a monitoring strategy for your cloud spend

SCCOST04-BP01 Use AWS services and advanced analytics to optimize overall supply chain costs

Consider using AWS Supply Chain to help optimize overall supply chain costs by taking advantage of pre-built features that are already optimized for cloud infrastructure cost efficiency.

Desired outcome: Use AWS Supply Chain to take advantage of pre-built features and which are already optimized for cloud infrastructure cost.

Benefits of establishing this best practice: Reduced cost, optimized performance, and better customer satisfaction.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

AWS Supply Chain's demand forecasting capabilities use machine learning to optimize inventory planning and mitigate over-stocking and stock-outs, enabling companies to maintain ideal inventory levels and minimize costs while supporting product availability.

AWS Supply Chain's data lake and visibility features help companies streamline operations, make more cost-effective inventory placement decisions, and optimize distribution by centralizing data from disparate systems to identify inefficiencies.

Implementation steps

1. Evaluate current supply chain processes to identify opportunities where AWS Supply Chain can provide cost optimization benefits.
2. Implement AWS Supply Chain's demand forecasting capabilities to optimize inventory planning and reduce carrying costs.
3. Use AWS Supply Chain's data lake and visibility features to identify operational inefficiencies and cost reduction opportunities.
4. Configure automated insights and collaboration capabilities to enable faster, more cost-effective supply chain decisions.
5. Monitor cost savings achieved through AWS Supply Chain implementation and identify additional optimization opportunities.
6. Continuously refine AWS Supply Chain configurations to maximize cost efficiency and operational performance.

SCCOST04-BP02 Implement a monitoring strategy for your cloud spend

Continually monitor and analyze usage patterns, network traffic, and associated costs to maintain optimal cost efficiency.

Desired outcome: A continuous improvement approach which uses lowest cost service options from Cloud to optimize cost.

Benefits of establishing this best practice: Reduced cost, optimized performance, and better customer satisfaction

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Define key cost metrics relevant to supply chain operations, such as data transmission costs, edge processing expenses, and cloud storage charges. Set budgets and alarms to Establish budget thresholds for each cost metric and configure alarms to notify when thresholds are approaching or exceeded, while regularly reviewing cost reports to identify anomalies, trends, or cost spikes that may require investigation or optimization.

Implementation steps

1. Define key cost metrics relevant to supply chain operations, including data transmission, processing, and storage costs.
2. Establish budget thresholds and configure automated alerts to notify when spending approaches or exceeds defined limits.
3. Implement regular cost review processes to identify spending trends, anomalies, and optimization opportunities.
4. Utilize AWS Trusted Advisor to receive recommendations for optimizing resource usage and reducing costs.
5. Apply cost-effective data management practices including retention policies, archival strategies, and deletion of obsolete data.
6. Track and optimize data transmission costs through techniques like data aggregation, compression, and prioritization.

Key AWS services

- AWS Cost Explorer
- AWS Budgets
- AWS Cost and Usage Report
- AWS Billing and Cost Management Conductor
- AWS Cost Anomaly Detection
- AWS Cost Categories
- AWS Billing and Cost Management Console
- Customer Carbon Footprint Tool
- AWS Billing and Cost Management and Cost Management and AWS Cost Allocation Tags
- AWS Cost Optimization Hub

Resources

- Monitoring tools in AWS for API Gateway
- AWS Solutions Library: Vetted solutions and guidance for Supply Chain business and technical use cases
- Trends Dashboard with AWS Cost and Usage Reports, Amazon Athena and Quick Suite
- Tagging AWS Resources and Tag Editor
- AWS Cloud Financial Management Blogs
- Cost Optimization Pillar - AWS Well-Architected Framework
- Overview of Data Transfer Costs for Common Architectures
- Using Amazon S3 Storage Lens to optimize your storage costs

Sustainability

The sustainability pillar provides design principles, operational guidance, best-practices, and improvement plans to meet sustainability targets for your Amazon Web Services workloads.

On average, two-third of companies' total greenhouse-gas emissions rely on their supply chains. For example, the typical consumer company's supply chain creates far greater social and environmental costs than its own operations, accounting for more than 80 percent of greenhouse-gas emissions and more than 90 percent of the impact on air, land, water, biodiversity, and geological resources.

Sustainability factors can also alter the growth projections of companies. Companies know that they will have to greatly reduce the natural and social costs of their products and services to capitalize on rising demand for them without taxing the environment or human welfare. Technology and cloud opportunities play a key role in this landscape as transitions to net-zero are relying on breakthrough innovations (for more information, see Fight Supply Chain Emissions to Fight Climate Change, AWS Sustainability, and Amazon Sustainability).

Most of the implementation guidance you can find in the Sustainability Pillar - AWS Well-Architected Framework is applicable in the supply chain space, and that guidance is referenced in this document when relevant. Some specific implementation guidance is provided through this lens due to the specific nature of supply chain workloads:

- On-premises workloads over different regions managing OT and IT at manufacturing sites, warehouses and fulfillment centers (FCs), distribution, sort centers, or logistics hubs.
- In the cloud, workloads across different Regions, sensors, and devices used for traceability purposes by logistic providers, and systems running across the suppliers' network.

A starting point is cloud sustainability, bringing with it the Shared Responsibility Model, the sustainability optimization reachable through the cloud, and the design principles for the sustainability in the cloud.

Focus areas

- Design principles
- Region selection
- Alignment to demand

Design principles

Supply chain operations rely on a complex technology landscape for the following key reasons:

- Geographical extension and coverage across the globe.
- Facilities geographically distributed requiring a mix of applications to run their operations.
- The number of products and services.
- Applications variety.
- Number of participants involved - internal and external - with their own systems to integrate with.

As companies are going through the process of optimizing their operations for sustainability, they recognize that the environmental impact is challenging but they also know that every apparently small detail and progress makes a significant change in reaching the sustainability targets. Companies need to adhere to environmental, social, and governance (ESG) standards to minimize environmental impact.

- **Structure for visibility over the supply chain network:** Structure your business and IT operations to collect the required visibility information over the entire supply chain network, comprising operations delivered through your own supply chain infrastructure and operations delivered by your partners, providers and carriers.
- **Monitor operations' performance across the organization with the supply chain SCOR model:** Monitor and measure supply chains business and IT operations performance through the supply chain operations reference (SCOR) model, providing a standard framework and a standard set of KPIs to build a common view, recognizable internally and externally, of your sustainability performance versus business and sustainability targets over plan, source, make, deliver, return, and enable model's areas.

- **Look at supply chain through the systems perspective:** Apply the systems perspective to your supply chains to look at your whole operations as an interconnected system, encompassing all stages, processes, and flows of materials, information, and resources. Applying this lens and perspective, it helps organizations to emphasize relationships, feedback loops among the different processes, stages, and parties. It also allows to identify, track and limit ripple effects, where changes or disruptions in one area can have effects able to spread and impact throughout the entire system.
- **Automate the data collection of sustainability-related information:** Automate ESG data collection like carbon emissions and greenhouse gas metrics by building integrations with partners like freight forwarders and transportation companies, where applicable:
  - All the time-consuming tasks to reduce the usage time of a required AWS resource, to collect data for peaks and valleys analysis to enable automatic scalability based on demand,
  - The provisioning of the AWS services you need to support your operations, to let them follow your business needs.
- **Design for on-demand over always-on, where possible:** To enhance your supply chain workloads on AWS, focus on improving your predictive capabilities for resource requirements. Use forecasts, seasonality patterns, and analyses of peaks and valleys to favor on-demand resources over always-on instances. This approach allows for more efficient resource management, whether you are turning resources on and off, scaling up and down, or scaling horizontally.
- **Align supply chain-related sustainability to company-wise sustainability goals:** Align supply chain workloads and the technology-related emissions to the wider organization's sustainability strategy and goals to enable the supply chain design, plan and execute for sustainability.

Region selection

SCSUS01: Can you optimize the AWS Regions where workloads should run to balance business needs and sustainability targets?

Optimizing AWS Region selection is crucial for supply chain operations because it directly impacts both operational performance and environmental sustainability by reducing latency, improving user experience, and minimizing carbon footprint through strategic placement of workloads.

SCSUS02: Can you optimize where your trading partners can consume required services based on supply chain network areas of execution?

Optimizing AWS Regions for trading partner access is considered important because it enables efficient global supply chain operations while minimizing environmental impact through strategic service placement and reduced data transmission requirements.

Best practices

- SCSUS01-BP01 Optimize your visibility over the entire supply chain network
- SCSUS02-BP01 Use the available AWS infrastructure to implement your distributed architecture

SCSUS01-BP01 Optimize your visibility over the entire supply chain network

Verify consistent visibility of your supply chain workloads across the entire supply chain network. The goal is to collect information on where workloads are running and how much resources they require to fulfill business needs. Reaching this level of visibility enables organizations to look for optimal AWS Regions, from both business efficiency and sustainability needs standpoint, where workloads can or should run to match service levels and sustainability targets.

Desired outcome: Achieve comprehensive visibility into your supply chain network, to help make sure that workloads are running within the optimal setup to meet business needs while minimizing emissions. This includes mapping critical workloads, highlighting self-managed areas versus partner areas and continuously adapting to the evolving business requirements and external conditions.

Benefits of establishing this best practice: This practice enables informed decision-making, optimal resource usage, and alignment of technology to sustainability targets. It promotes transparency across supply chain networks, which enhances accountability and performance efficiency.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Evaluate and map your supply chains technology-related workloads, focusing especially on the most critical scenarios, with your supply chain network. This creates a comprehensive view of where you run the most intensive workloads, where you have the biggest facilities or most relevant supply chain infrastructures, and how they connect to each other through the network.

Highlight the areas of your network which are directly managed by you and which ones from your trading partners, while considering calculating the footprint of the workloads running on-premises and in the cloud.

Implementation steps

1. Map supply chain technology workloads and identify the most critical scenarios across your network infrastructure.
2. Evaluate current workload placement and calculate emissions footprint for both on-premises and cloud-based operations.
3. Assess optimal AWS Regions based onProximity to renewable energy projects in the regions, lowest carbon footprint, latency requirements, and service availability.
4. Analyze cost implications and Sovereignty constraints when selecting AWS Regions for workload placement.
5. Develop a migration plan for workloads that should be moved to more sustainable AWS Regions while maintaining operational requirements.
6. Establish ongoing monitoring and optimization processes to adapt AWS Region selection as business needs and sustainability goals evolve.

SCSUS02-BP01 Use the available AWS infrastructure to implement your distributed architecture

Consider optimizing where you run your workloads using the extensive AWS infrastructure and a distributed architecture to enable your trading partners to rely on services based on their predominant areas of operation.

Desired outcome: Enable seamless execution of supply chain operations by optimizing workload distribution across appropriate AWS Regions, matching partners needs and aligning with sustainability and operational goals.

Benefits of establishing this best practice: Optimizes the emissions while supporting global scalability, latency and performance. It serves also as a practice to align sustainability targets with trading partners' operations, facilitating also the dynamic, on-demand resource scaling to reach optimal cost and performance ratio.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Evaluate a distributed architecture to support your supply chain operations, using the extensive AWS infrastructure. Consider mapping the optimal AWS Regions, correlating from where your trading partners could benefit the execution from, while using the scaling capabilities of the AWS infrastructure to replicate services where needed and adopt an on-demand approach with related automations to scale, turn on and off services based on target areas of execution.

Implementation steps

1. Map trading partner locations and their predominant areas of supply chain execution to identify optimal region placement.
2. Evaluate distributed architecture options that use AWS infrastructure to support global supply chain operations.
3. Implement AWS region-specific service deployments that align with partner operational areas and sustainability goals.
4. Configure automated scaling and on-demand resource provisioning based on regional demand patterns.
5. Establish monitoring and optimization processes to facilitate efficient resource utilization across distributed AWS Regions.
6. Regularly review and adjust regional deployments based on changing partner needs and sustainability targets.

Alignment to demand

SCSUS03: Can you align your planning, execution, and enablement operations to the actual demand to optimize the emissions?

Aligning supply chain operations to actual demand is essential for sustainability because it minimizes waste, reduces unnecessary resource consumption, and optimizes emissions by making sure resources are used only when and where needed.

Best practices

- SCSUS03-BP01 Use the supply chain operations reference (SCOR) to map your supply chain

SCSUS03-BP01 Use the supply chain operations reference (SCOR) to map your supply chain

Consider the adoption of the SCOR model or equivalent standardized models like Value Reference Model (VRM) and managing for supply chain performance (M4SC) to map your supply chains and keep related metrics monitored, to be sure you are aligning planning, execution and enablement to the actual demand, leading to emissions optimizations.

Desired outcome: Develop a structured, measurable, and adaptable view of your supply chain to align operations with actual demand, help minimize emissions, and optimized resource use.

Benefits of establishing this best practice: Provides a standardized framework for monitoring and improving supply chain operations, leading to reduced waste, better alignment with sustainability targets, and increased agility.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Evaluate the adoption of the SCOR model over the organization to generate an aggregated view of your operations, the implemented use cases, and the related technology workloads, considering the six areas of the model: plan, source, make, deliver, return, enable. This would allow your organization to rely on a common model to keep tracking and measuring technology services, use cases and related operations you run and where (location), your performance and emissions your operations generate, while using tags applied to the AWS services in use for straightforward report, export, and aggregated views.

Implementation steps

1. Adopt the SCOR model or equivalent standardized framework to map and categorize your supply chain operations.

2. Implement comprehensive tagging strategies for AWS services to enable the tracking by SCOR model areas and Supply Chain network locations.
3. Establish metrics and monitoring systems to track performance and emissions across all SCOR model areas.
4. Create aggregated views that show the percentage of operations running in cloud versus on-premises for each supply chain area of the model.
5. Identify and plan migration strategies for the services corresponding to the on-premises percentage that you would move to the cloud to gain additional sustainability benefits.
6. Regularly review and update the map of your supply chain to reflect changes you might have applied to your operations, and to get an updated status of where you are towards your sustainability targets.

Software and architecture

SCSUS04: Can you optimize your compute workloads for your supply chain sustainability?

Optimizing compute workloads for sustainability is crucial because it directly impacts energy consumption and carbon emissions while maintaining the performance and reliability required for effective supply chain operations.

Best practices

- SCSUS04-BP01 Optimize your compute workloads for your supply chain sustainability
- SCSUS04-BP02 Build and run optimization models for resources involved in supply chains sustainability

SCSUS04-BP01 Optimize your compute workloads for your supply chain sustainability

Consider configuring AWS Compute Optimizer to analyze and investigate supply chain sustainability related workloads, to support your analysis on how to optimize the usage of compute resources to sustain your supply chain workloads.

Desired outcome: Optimize the performance of compute workloads to reduce energy consumption and emissions while maintaining the reliability of supply chain operations.

Benefits of establishing this best practice: Enhances the efficiency of compute resource utilization, reduces operational costs, and aligns sustainability efforts with performance objectives.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Before proceeding with scenarios simulation over your supply chains operations, to help you understand why and which set of operations are requiring more compute and memory resources, consider to setup and run AWS Compute Optimizer combined with Amazon CloudWatch metrics to analyze resource utilization patterns and identify optimization opportunities, leading as a direct consequence to sustainability's KPIs improvements.

Implementation steps

1. Configure AWS Compute Optimizer to analyze supply chains workload performance and resource utilization patterns.
2. Provision Amazon CloudWatch and configure metrics collection to gather detailed performance data across all supply chains compute resources.
3. Analyze compute utilization patterns to identify over-provisioned or under-utilized resources that can be optimized.
4. Right-size compute instances based on actual usage patterns and performance requirements.
5. Implement automated scaling policies to match compute resources with actual demand patterns.
6. Monitor and measure the impact of optimization efforts on both performance and sustainability metrics.

SCSUS04-BP02 Build and run optimization models for resources involved in supply chains sustainability

Consider building and run specific optimization models targeting supply chains sustainability, through scenarios simulation able to simulate resources usage and collect metrics for supply chains planning, execution and enablement.

Desired outcome: Develop and use optimization models to identify opportunities for operations efficiency, resource efficiency, reduce emissions, and align resource usage with both sustainability and business objectives.

Benefits of establishing this best practice: Facilitates data-driven resource allocation, helps with optimal performance with minimal environmental impact, and supports comprehensive scenario planning for supply chain operations.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Optimization models specifically envisioned for supply chain sustainability can be designed, built, and configured through optimization capabilities running on AWS as managed services.

This allows you to optimize your operations and the use of resources to achieve lower CO2 emissions and energy optimization, while generating more efficient purpose-built analysis for sustainability. The integration of these sustainability measures with existing optimization analysis enables greater focus on cost efficiency, service-level performance, and the ability to respond to disruptions or failures.

Implementation steps

1. Design and develop optimization models specifically focused on supply chain sustainability using AWS managed services.
2. Integrate sustainability Software and architecturemetrics with existing cost efficiency and performance optimization models.
3. Implement scenario simulation capabilities to test different resource allocation strategies and their sustainability impact.
4. Configure automated optimization workflows that balance sustainability goals with operational efficiency and requirements.
5. Establish feedback loops to continuously improve optimization models based on actual performance and sustainability outcomes.
6. Create reporting and visualization tools to communicate optimization results and sustainability improvements to stakeholders.

Data management

SCSUS05: How does your data strategy support your sustainability outcomes?

A well-designed data strategy is fundamental to achieve sustainability outcomes because it enables efficient data collection, processing, and analysis while minimizing resource consumption and supporting informed decision-making for environmental goals.

SCSUS06: How do you exchange data with trading partners to efficiently reach higher levels of compliance?

Efficient data exchange with trading partners is essential for sustainability compliance because it enables transparent reporting, collaborative sustainability initiatives, and adherence to evolving environmental regulations across the supply chain network.

Best practices

- SCSUS05-BP01 Adopt modern data management and governance practices for your supply chain sustainability, and focus on economic, environmental, and social needs
- SCSUS06-BP01 Enhance your data strategy and exchange capabilities with your trading partners

SCSUS05-BP01 Adopt modern data management and governance practices for your supply chain sustainability, and focus on economic, environmental, and social needs

Consider supply chain fine-tuned data lake, analytics, and data governance practices with specific focus on sustainability to address economic, environmental and social needs.

Desired outcome: Implement robust data management practices to help with sustainability-related use cases, providing support for accurate, secure, and comprehensive datasets.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Consider the adoption of a managed supply chain fine-tuned data lake using Amazon S3, and Amazon S3 Tables and table bucket, for unmatched performance, durability, availability, scalability, security, compliance and audit capabilities, in combination with AWS Lake Formation to accelerate the build of secure data lakes. Build your data inventory considering all the data sources (both internal and external), your EDI flows, and create your data catalog with the proper metadata and tags that can help you map which information is contributing to both the economic, environmental and social needs perspectives.

Implementation steps

1. Implement a managed supply chain data lake using Amazon S3, Amazon S3 Tables and table buckets, and AWS Lake Formation to centralize sustainability-related data.
2. Build a comprehensive data inventory that includes internal and external data sources, EDI flows, and sustainability metrics.
3. Create detailed data catalogs with metadata and tags that map data contributions to economic, environmental, and social sustainability needs.
4. Implement data governance policies and access controls to maintain data quality and security across the sustainability data environment.
5. Establish data integration pipelines that connect AWS Glue with Amazon DataZone for comprehensive data management across organizational boundaries.

SCSUS06-BP01 Enhance your data strategy and exchange capabilities with your trading partners

Consider enhancing your data strategy and your data exchange capabilities with external parties and trading partners or providers to address compliance needs (for example, digital product passport, battery passport, and CO2 emissions reports) and to accelerate the path towards your sustainability targets.

Desired outcome: Foster collaboration and compliance across the supply chain by adopting decentralized data exchange strategies (like data spaces) and enhancing data-sharing capabilities.

Benefits of establishing this best practice: Accelerates the achievement of sustainability targets and needs through increased transparency and improved compliance.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Strengthen your data strategy for supply chain and sustainability use cases, and more generally, for the entire organization. If already not in place, consider allocating time and resources to the development of your data strategy, while considering the adoption of decentralized approaches (for example, data spaces) applied to data exchange, to efficiently steer towards adhering to regulations to reach higher levels of compliance and simplify the implementation of use cases that require complex data exchange over the trading partners network.

Implementation steps

1. Develop a comprehensive data strategy that encompasses supply chain sustainability use cases and organizational requirements.
2. Evaluate and implement decentralized data exchange approaches (data spaces) to facilitate trading partner data sharing.
3. Establish secure data sharing protocols that support compliance requirements, such as digital product passport and battery passport.
4. Configure automated CO2 emissions reporting capabilities that integrate with trading partner systems.
5. Implement data governance frameworks that maintain compliance with sustainability regulations across partner networks.
6. Create monitoring and auditing capabilities to track data exchange effectiveness and compliance adherence.

Hardware and services

SCSUS07: Do you plan and design your supply chain and sustainability needs for automation?

Planning and designing for automation in supply chain sustainability is crucial because it reduces manual processes, optimizes resource utilization, and enables dynamic scaling that aligns with actual demand patterns while minimizing environmental impact.

SCSUS08: Are you designing the architecture for your resources for on-demand over always-on?

Designing architecture for on-demand resource usage rather than always-on is essential for sustainability because it significantly reduces energy consumption and carbon emissions by making sure resources are only active when needed.

Best practices

- SCSUS07-BP01 Plan and design for automation for supply chain sustainability
- SCSUS08-BP01 Collect usage data to feed advanced analysis and ML models to better predict future resources needs

SCSUS07-BP01 Plan and design for automation for supply chain sustainability

Consider optimizing your supply chain sustainability through automation, planning, and designing for automation. Plan for designing completely or partially, where applicable, all the time-consuming tasks to reduce the usage time of a required AWS resource, to collect data for peaks and valleys analysis to feed them into ML models or advanced analysis to enable automatic scalability based on demand.

Provision the AWS Cloud services you need to support your operations based on your business needs.

Desired outcome: Streamline supply chain operations through automation, reducing manual processes, and optimizing resource utilization to align with sustainability goals.

Benefits of establishing this best practice: Enhances operational efficiency, reduces costs, and improves responsiveness to changing business needs.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Automate the provisioning of the AWS services you need to support your operations to keep the technology infrastructure quickly adjustable in case your business needs change. Automation is a

best practice in the context of supply chain and sustainability, as well as implementing predictive horizontal and vertical scaling of compute resources, turning on and off resources based on usage and demand, and forecasting the demand, business peaks and valleys due to seasonality, and promotions for direct and indirect emissions optimization.

Implementation steps

1. Implement infrastructure as code (IaC) approaches to automate the provisioning and management of AWS services supporting supply chain operations.
2. Configure predictive scaling policies for compute resources based on historical demand patterns and seasonality analysis.
3. Establish automated resource scheduling to turn resources on/off based on actual usage patterns and business demand.
4. Deploy machine learning models to forecast demand patterns and optimize resource allocation for sustainability.
5. Implement automated monitoring and alerting systems to track resource utilization and sustainability metrics.
6. Create continuous improvement processes to refine automation strategies based on performance and sustainability outcomes.

SCSUS08-BP01 Collect usage data to feed advanced analysis and ML models to better predict future resources needs

Consider improving your ability to predict AWS Cloud resources required for your supply chain and sustainability-related workloads to prefer on-demand over always-on. Base this data on forecasts, seasonality, and peaks and valleys analysis to efficiently turn resources on and off accordingly or scaling resources up and down and horizontally.

Desired outcome: Achieve dynamic scalability and resource efficiency by using historical usage data to predict and optimize resource needs.

Benefits of establishing this best practice: Improves operational agility, reduces downtime, and minimizes unnecessary resource usage.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Consider collecting data about resource usage over the past years to design and prefer on-demand over always-on, with the main goal of optimizing resources scaling, uptime and downtime, availability, and replication based on your business needs.

Gain visibility of required resources through ML-based predictions, using built-in features of AWS System Manager, Instance Scheduler on AWS, and signals from Amazon CloudWatch, while using managed databases like Amazon RDS, and containers orchestration running on AWS towards serverless architectures.

Implementation steps

1. Collect and analyze historical resource usage data to identify patterns and optimization opportunities for on-demand resource allocation.
2. Implement machine learning-based prediction models to forecast future resource needs based on business patterns and seasonality.
3. Deploy AWS Systems Manager and Instance Scheduler to automate resource scheduling based on predicted demand patterns.
4. Configure Amazon CloudWatch monitoring to provide real-time signals for dynamic resource scaling decisions.
5. Migrate appropriate workloads to managed databases and serverless architectures to optimize resource utilization.
6. Establish continuous monitoring and optimization processes to refine on-demand resource strategies over time.

Process and culture

SCSUS09: Do you align your supply chain sustainability metrics with company-wise mid/long-term sustainability goals?

Aligning supply chain sustainability metrics with company-wide goals is critical because it facilitates coordinated efforts, maximizes impact, and provides clear accountability for environmental performance across the entire organization.

SCSUS10: Are you using document digitization to reduce paper waste and align with your ESG and sustainability goals?

Using document digitization is important for sustainability because it significantly reduces paper consumption, alleviates physical storage requirements, and enables more efficient data sharing while supporting broader ESG objectives.

Best practices

- SCSUS09-BP01 Align your supply chain sustainability goals and metrics with the broader set of company-wise sustainability goals
- SCSUS10-BP01 Use document digitization as an ESG goal

SCSUS09-BP01 Align your supply chain sustainability goals and metrics with the broader set of company-wise sustainability goals

Align supply chain workloads and the technology-related emissions to the wider organization's sustainability strategy and goals to monitor how their impact evolves over the time and contributes to your organization's sustainability targets.

Desired outcome: Supply chain sustainability initiatives contribute effectively to the overall sustainability goals of the organization.

Benefits of establishing this best practice: Creates a unified approach to sustainability, enhances organizational impact, and helps with consistent progress toward long-term goals.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Supply chains are almost always responsible for most of the emissions produced by an organization, but this is true considering all the supply chains involved to plan, source, make, deliver and, eventually, return a product or component. Technology-related workloads are responsible of only a portion of the total emissions, but depending on how much your organization is digitized, the percentage can vary and emit a larger portion compared to overall emissions. The adoption of the cloud to run all or partially your operations eases the tracking and measuring

carbon emissions with regards to your AWS-related workloads through the Customer Carbon Footprint tool.

Implementation steps

1. Establish clear alignment between supply chain sustainability metrics and company-wide sustainability goals and targets.
2. Implement the Customer Carbon Footprint tool to track and measure carbon emissions from AWS-related supply chain workloads.
3. Create regular reporting mechanisms that show how supply chain sustainability initiatives contribute to overall organizational goals.
4. Establish governance processes to make sure supply chain sustainability efforts are coordinated with broader organizational sustainability strategies.
5. Monitor and measure the percentage impact of technology-related emissions within the overall organizational carbon footprint.
6. Develop continuous improvement processes to enhance the contribution of supply chain sustainability to company-wide goals.

SCSUS10-BP01 Use document digitization as an ESG goal

Explore opportunities to digitize any physical documentation used for supply chain operations within the company but also in operations involving partners and external entities. Digitization of physical documentation leads to a positive ripple effect over sustainability-related use cases, simplifying data sharing across companies and supply chains, data transparency, and solutions required to solve compliance-related needs.

Desired outcome: Avoid or significantly reduce the use of physical documentation in supply chain operations, leading to measurable reductions in paper waste, improved data accessibility, and alignment with sustainability goals.

Benefits of establishing this best practice:

- **Environmental benefits:** Reduces paper waste, lowering the organization's carbon footprint and aligning with ESG objectives.
- **Operational benefits:** Improves document accessibility, reduces processing time, and enhances data-driven decision-making.

- **Compliance benefits:** Enables better tracking, management, and storage of sensitive supply chain data in secure, auditable digital formats.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Supply chain operations often generate significant volumes of physical documents, including supplier contracts, freight airway bills (AWBs), and invoices. Transition to a digital-first approach by using AI-powered document digitization tools, such as Amazon Textract and AWS Comprehend, to extract, organize, and analyze data from physical documents. Integrate these tools into your supply chain workflows to minimize paper dependency, while evaluating the environmental impact of physical documentation and quantifying the reductions achieved through digitization initiatives.

Implementation steps

1. Identify all physical documentation used in supply chain operations and assess opportunities for digitization.
2. Implement AI-powered document digitization tools such as Amazon Textract and AWS Comprehend to automate document processing.
3. Create digital repositories for centralized document management using secure AWS storage services.
4. Establish Secure and compliance-aligned document storage using AWS tools like Amazon S3 and AWS KMS.
5. Automate document processing workflows to improve operational efficiency and minimize paper dependency.
6. Measure and report on environmental impact reductions achieved through digitization initiatives to support ESG goals.

Key AWS services

- Customer Carbon Footprint tool
- Solutions for Manufacturing and Industrial
- Building data spaces for sustainability use cases
- AWS Supply Chain

- Instance Scheduler on AWS

Resources

- Sustainability Resources
- Amazon - Sustainability in the Cloud
- Amazon - Renewable Energy Methodology
- AWS Sustainability
- How moving onto the AWS cloud reduces carbon emissions
- AWS Solutions Library for sustainability

Conclusion

The Supply Chain Lens provides architectural best practices across the six pillars for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud. The lens provides a set of questions that allows you to review an existing or proposed architecture, as well as a set of supply chain best practices for each pillar. Using the Framework in your Supply Chain architecture helps you produce stable and efficient systems, which allow you to focus on your functional requirements.

Contributors

The following individuals and organizations contributed to this document:

- Sunil Vishnubhotla, Senior Technical Account Manager, AWS Enterprise Support, Amazon Web Services
- Maurice Stratton, Supply Chain Transformation Advisor, Amazon Web Services
- Sanjeev Kumar, Senior Technical Account Manager, AWS Enterprise Support, Amazon Web Services
- Mohan Udyavar, Principal Technical Account Manager, AWS Enterprise Support, Amazon Web Services
- Daniel Aucoin, Senior Solutions Architect, Amazon Web Services
- Nikhil Lalla, Senior ProServe Cloud Architect, Amazon Web Services
- Dhinakar Ramamurthy, Global Solutions Architect, Amazon Web Services
- Ali Zagros, Senior Solutions Architect, Amazon Web Services
- Sujoy Gulati, Senior Technical Account Manager, AWS Enterprise Support, Amazon Web Services
- Mahesh Geeniga, Senior Partner Solutions Architect, Amazon Web Services
- Gianenrico Salerno, WW Tech Leader Mfg and SC, CoE Manufacturing and Supply Chain, Amazon Web Services
- Mais Rihani, Senior PCA Manager, Amazon Web Services
- Glenn Mendonca, Product Manager, Amazon Web Services
- Bruce Ross, Well-Architected Lens Lead, Solutions Architect, Amazon Web Services
- Jun-Tin Yeh, Senior Solutions Architect, Amazon Web Services
- Mahmoud Matouk, Principal Security Lead SA, Amazon Web Services
- Ryan Dsouza, Principal Guidance Lead SA, Amazon Web Services
- Arvind Raghunathan, Principal Operations Lead SA, Amazon Web Services
- Madhuri Srinivasan, Sr. Technical Writer, Amazon Web Services
- Stewart Matzek, Sr. Technical Writer, Amazon Web Services
- Matthew Wygant, Sr. TPM Guidance, Amazon Web Services

Document revisions

Change	Description	Date
Initial release	Initial release of the Supply Chain Lens.	September 9, 2025

AWS Glossary

For the latest AWS terminology, see the AWS glossary in the *AWS Glossary Reference*.