

Securing the Supply Chain in a Digital Age

Ricky Allen
February 23, 2025



©2025 CyberOne LLC. All rights reserved.

Our Dependency on Supply Chain

Our dependency on complex, interconnected global supply chains has cast a dark shadow over the cybersecurity landscape, leaving organizations more vulnerable than ever before. As we hurtle towards a future where 45% of organizations worldwide are expected to fall victim to software supply chain attacks by 2025. The cascading effect of these attacks is nothing short of catastrophic, with a single breach having the potential to compromise millions of users and cripple entire industries. The fact that 98% of organizations have already felt the sting of supply chain breaches.

This session provides a self evaluation and seven steps for process improvement regarding your Supply Chain.



Speaker Introduction

Ricky Allen

Ricky Allen is the VP of Strategy and Solutions for CyberOne Security, an ISSA Fellow and Past-President of the South Texas ISSA chapter. He holds certifications such as SABSA Security Architecture, CISSP, CISA, and Six Sigma.

Ricky has 25 years of cybersecurity experience with previous roles as a founder at Critical Start, Accenture in their strategic information security consulting practice and at HP Enterprise Security Products as the practice lead for developing Security Operations programs.

Ricky has presented at conferences such as BSides, Black Hat, ISSA, ISACA, API Cybersecurity, HOU.SEC.CON, RSA, SANS, SecureWorld, Data Connectors, and most importantly – IWS of Oklahoma.



Supply Chain Management

Core Initiative for Security

- Supply Chain Security Management is a critical aspect of modern business operations that focuses on identifying, evaluating, and mitigating risks associated with the entire network of resources, processes, and partnerships involved in the production and distribution of goods and services

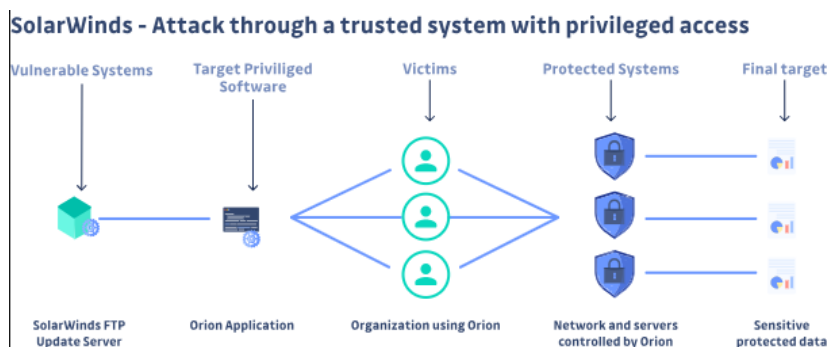


Supply Chain Vulnerabilities

Increasing complexity and digitalization of supply chains along with rising cybersecurity threats have exposed numerous intellectual property risks leading to overall supplier reliability concerns.

SolarWinds Hack

- One of the most significant supply chain attacks in recent history
- Affected U.S. government agencies and Fortune 500 companies
- Malicious code inserted into software updates
- Distributed to approximately 18,000 customers



Japan Aviation Electronics (JAE) Cyber Attack

- Major aerospace and electronics manufacturer targeted in 2023
- ALPHV/BlackCat ransomware group responsible
- Operational disruptions, including website and email issues
- Highlights risks to critical infrastructure in electronics sector

The Changing Landscape of Supply Chain Security

- Increasing reliance on digital technologies
- Global nature of supply chains
- Rising sophistication of cyber threats
- Regulatory changes and compliance requirements

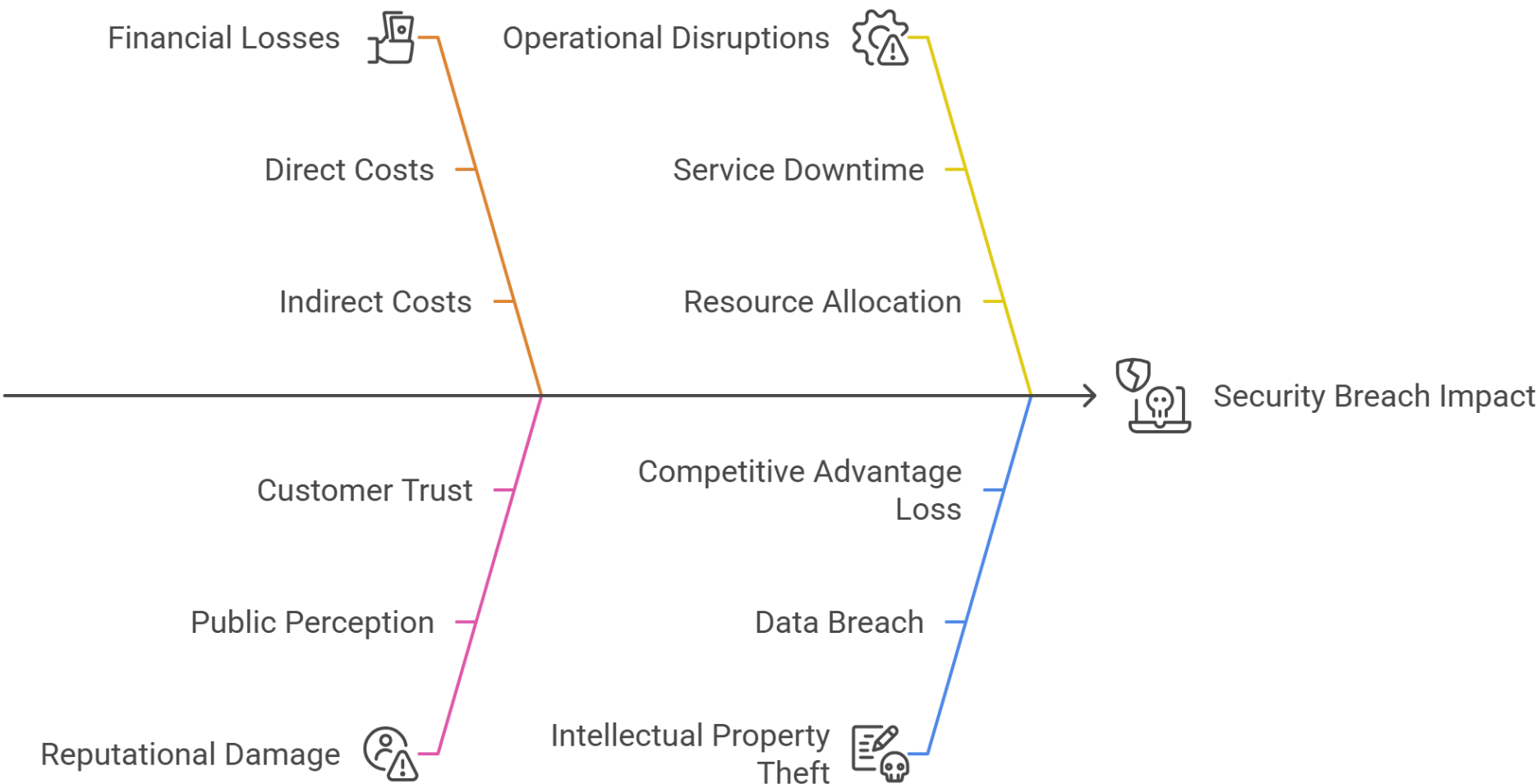


Key Challenges in Electronics Supply Chain

- Component shortages with lead times for semiconductions extending to up to 30 weeks
- Supply chain disruptions (e.g., pandemics, natural disasters)
- Rising component costs from transportation and labor costs
- Cybersecurity threats from very sophisticated nation state attackers
- Geopolitical tensions, tariffs, and regulatory challenges
- Lack of supply chain visibility related to real time inventory and risk management
- Supplier reliability and dependence on rapidly changing technology capabilities
- Volatility of electronics that require specific handling requirements

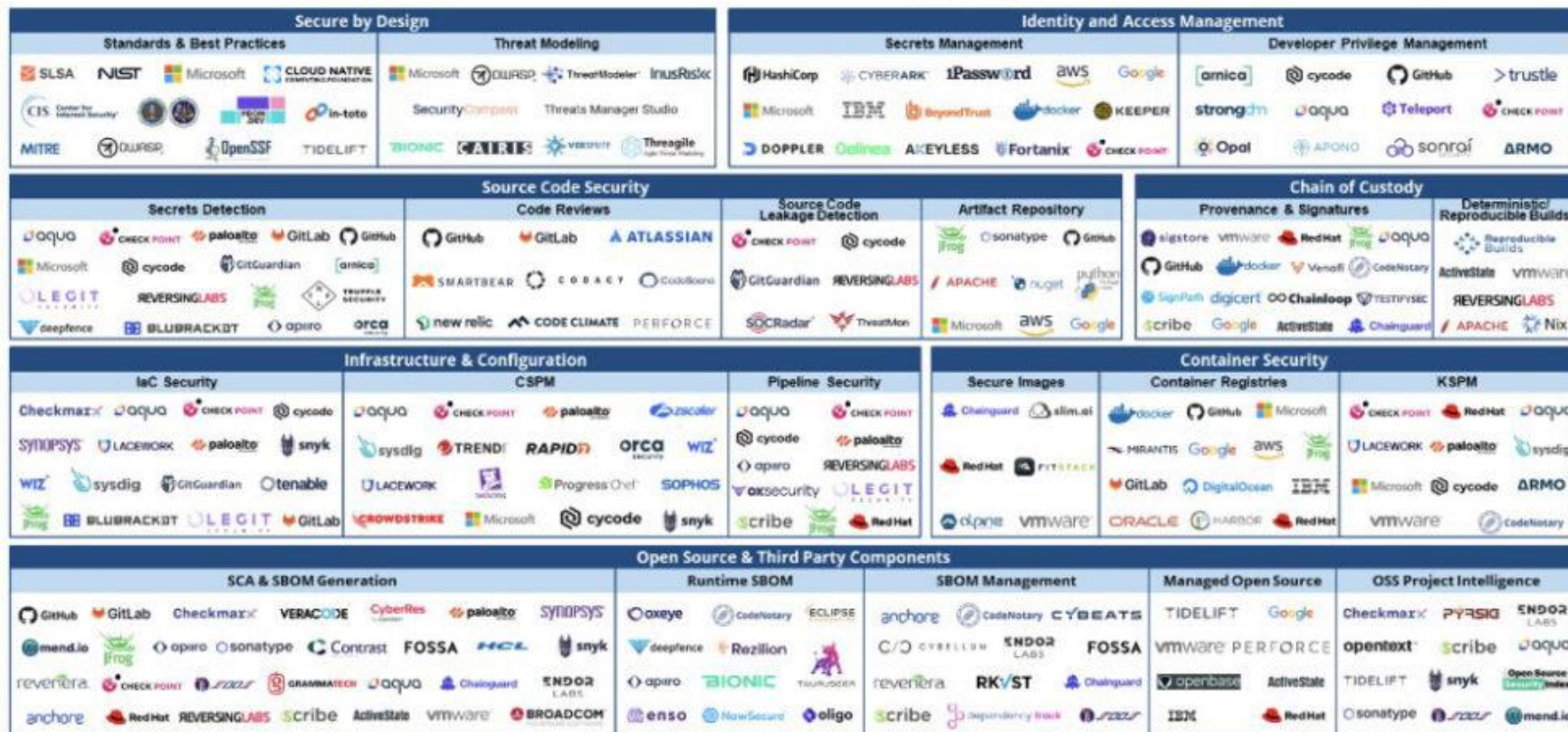


Evaluating the Impact of Supply Chain Breaches



Can I just buy a software product for this?

IDC Market Glance: Software Supply Chain Security



Source: IDC, 2Q23

For areas on which IDC publishes market share data, the top 3-5 market share leaders are represented.
For areas on which IDC does not publish market share data, vendor selection is up to analyst discretion.



© IDC | 2



Self Evaluation



©2025 CyberOne LLC. All rights reserved.

Self Evaluation

QUIZ

1. How would you rate your organization's current understanding of supply chain security risks in the electronics industry? a) Very limited understanding b) Basic understanding of some risks c) Good understanding of most risks d) Comprehensive understanding of all major risks
 2. Which aspect of supply chain security do you believe will be most challenging to implement in your organization? a) Implementing robust access control and authentication measures b) Conducting thorough vendor risk assessments and due diligence c) Encrypting sensitive data throughout the supply chain d) Establishing effective incident response and recovery procedures
 3. How many of the following supply chain security measures has your organization implemented or plans to implement within the next month?
 - Conducting regular security audits of suppliers
 - Implementing multi-factor authentication for supply chain systems
 - Establishing a formal incident response plan for supply chain disruptions
 - Encrypting sensitive data shared with suppliers
 - Providing cybersecurity training specific to supply chain risks
- a) None of these measures b) 1-2 of these measures c) 3-4 of these measures d) All 5 of these measures



Self Evaluation

QUIZ

4. How confident do you feel in your ability to conduct a basic risk assessment of your organization's supply chain? a) Not confident at all b) Somewhat confident, but need more information c) Confident in conducting a basic assessment d) Very confident, can conduct a comprehensive assessment
5. Considering the case studies presented (SolarWinds and Japan Aviation Electronics), how many similar vulnerabilities can you identify in your own organization's supply chain? a) None b) 1-2 vulnerabilities c) 3-4 vulnerabilities d) 5 or more vulnerabilities
6. How well do you understand the role of encryption in securing supply chain data? a) Limited understanding b) Basic understanding c) Good understanding d) Expert-level understanding
7. Which strategy do you think will be most effective in building a culture of security within your organization? a) Regular security awareness training b) Implementing strict security policies c) Offering incentives for secure behavior d) Leading by example from top management
8. How prepared do you feel to integrate suppliers into your organization's security protocols? a) Not prepared at all b) Somewhat prepared, but need guidance c) Well prepared for most suppliers d) Fully prepared to integrate all suppliers



Self Evaluation

QUIZ

9. Regarding continuous monitoring and assessment, which tools or processes do you think your organization needs to implement or improve most urgently? a) Real-time threat detection systems b) Regular security audits c) Automated vulnerability scanning d) Incident response planning
10. How has this workshop changed your perspective on the importance of supply chain security in the electronics industry? a) No change in perspective b) Slightly more aware of its importance c) Significantly more aware and planning some changes d) Completely transformed perspective, planning major changes



Answer Key and Scoring Bands

To determine the maturity of your organization's supply chain security, use the following scoring system: For each question, assign points based on the answer: a) 1 point b) 2 points c) 3 points d) 4 points

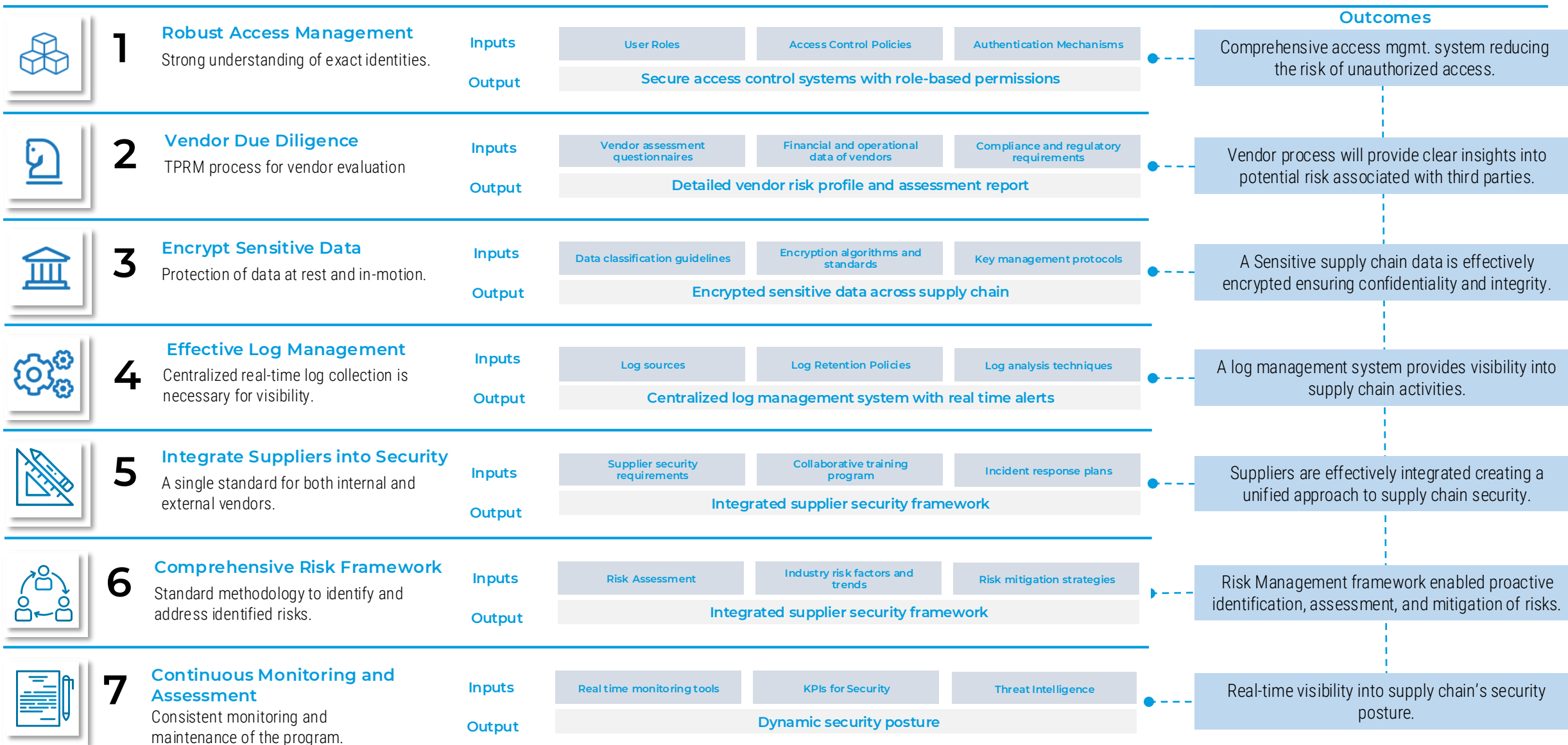
Total Score Interpretation:

- 10-20 points: Initial Stage
 - 21-30 points: Developing Stage
 - 31-35 points: Established Stage
 - 36-40 points: Advanced Stage
1. Maturity Levels: Initial Stage (10-20 points): Your organization is in the early stages of understanding and implementing supply chain security measures. There's a significant need for improvement across all areas.
 2. Developing Stage (21-30 points): Your organization has a basic understanding of supply chain security and has implemented some measures. However, there are still considerable gaps that need to be addressed.
 3. Established Stage (31-35 points): Your organization has a good grasp of supply chain security principles and has implemented many best practices. There's room for refinement and advancement in specific areas.
 4. Advanced Stage (36-40 points): Your organization demonstrates a high level of maturity in supply chain security. You have comprehensive measures in place and are well-prepared to handle most security challenges.



Plan for Addressing Supply Chain Security

Electronic Supply Chain- the following seven steps will help reduce risk to the organization.





Implementing robust access management involves establishing strict controls over who can access various resources and data within the supply chain network, ensuring only authorized personnel have access to sensitive information

Recommended Actions:

- **Enforce Identity and Access Management (IAM) solutions:** Implement comprehensive IAM systems to manage user identities and access rights across the supply chain.
- **Utilize Multi-Factor Authentication (MFA) for critical systems:** Require multiple forms of verification before granting access to sensitive systems or data.
- **Implement Role-Based Access Control (RBAC) :** Assign access rights based on job roles to ensure users only have access to necessary resources.
- **Conduct regular access reviews and updates:** Periodically review and update access rights to maintain the principle of least privilege.
- **Monitor and analyze access logs continuously:** Use automated tools to track and analyze user access patterns for anomaly detection.
- **Implement least privilege principles:** Grant users the minimum level of access required to perform their job functions.
- **Establish strong password policies:** Enforce complex password requirements and regular password changes.
- **Use Single Sign-On (SSO) for streamlined access:** Implement SSO to reduce the number of credentials users need to manage while maintaining security.

Outcomes

Comprehensive access mgmt. system reducing the risk of unauthorized access.

- **Improved compliance with regulatory requirements:** Meets industry standards and legal obligations for data protection.
- **Reduced insider threats:** Limits the potential for internal misuse of sensitive information.
- **Increased operational efficiency:** Streamlines access processes, reducing time spent on manual access management.
- **Better incident response capabilities:** Enables quick identification and containment of security incidents.
- **Strengthened trust with supply chain partners:** Demonstrates commitment to protecting shared data and resources.
- **Scalability and flexibility in access management:** Adapts to changing organizational needs and user roles.
- **Improved accountability and traceability of user actions:** Provides clear audit trails for all access activities.



Outcomes

Vendor process will provide clear insights into potential risk associated with third parties

Conducting thorough vendor due diligence involves a comprehensive assessment of potential vendors to identify and mitigate risks associated with financial stability, legal compliance, operational efficiency, and cybersecurity practices.

Recommended Actions:

- **Perform financial assessments of vendors:** Evaluate vendors' financial health to ensure long-term stability and reliability.
- **Verify legal compliance with relevant laws and regulations:** Ensure vendors adhere to applicable industry standards and legal requirements.
- **Evaluate operational capabilities and business continuity plans:** Assess vendors' ability to maintain operations during disruptions.
- **Assess vendors' cybersecurity measures and practices:** Review vendors' security policies, procedures, and technologies.
- **Implement regular audits and ongoing monitoring:** Conduct periodic checks to ensure continued compliance and security.
- **Review vendors' data protection policies:** Examine how vendors handle, store, and protect sensitive information.
- **Examine vendors' incident response plans:** Evaluate vendors' preparedness for potential security breaches or disruptions.
- **Conduct on-site visits and inspections:** Physically verify vendors' security measures and operational practices.

- **Risk mitigation in vendor relationships:** Identifies and addresses potential vulnerabilities before they become issues.
- **Ensured regulatory compliance:** Maintains adherence to industry standards and legal requirements.
- **Enhanced overall security posture:** Strengthens the entire supply chain by addressing weak links.
- **Informed decision-making in vendor selection:** Provides comprehensive data for choosing the most suitable vendors.
- **Improved operational continuity:** Reduces the likelihood of disruptions due to vendor issues.
- **Stronger and more reliable vendor partnerships:** Builds trust and transparency in vendor relationships.
- **Cost efficiency through avoided non-compliance issues:** Prevents potential fines and penalties associated with regulatory violations.
- **Reduced likelihood of supply chain disruptions:** Minimizes the risk of unexpected vendor-related interruptions.



3 Encrypt Sensitive Data

Protection of data at rest and in-motion.

Inputs

Data classification guidelines

Encryption algorithms and standards

Key management protocols

Output

Encrypted sensitive data across supply chain

Outcomes

A Sensitive supply chain data is effectively encrypted ensuring confidentiality and integrity:

Encrypting sensitive data in supply chain contexts involves securing information both at rest and in transit, using robust encryption methods to safeguard against potential breaches and data leaks.

Recommended Actions:

- **Encrypt data at rest and in transit:** Apply encryption to data stored in databases and during transmission between systems.
- **Implement Data Loss Prevention (DLP) solutions:** Deploy tools to detect and prevent unauthorized data transfers.
- **Use strong cryptographic methods:** Employ industry-standard encryption algorithms and key lengths.
- **Regularly update encryption protocols:** Stay current with the latest encryption standards and best practices.
- **Conduct security audits of encryption practices:** Periodically review and test the effectiveness of encryption measures.
- **Implement key management systems:** Establish secure processes for generating, storing, and rotating encryption keys.
- **Train employees on proper data handling and encryption procedures:** Educate staff on the importance of encryption and correct data handling practices.
- **Implement end-to-end encryption for sensitive communications:** Ensure that data remains encrypted throughout its entire journey in the supply chain.

- **Compliance with data protection regulations:** Meets legal requirements for safeguarding sensitive information.
- **Improved trust with supply chain partners:** Demonstrates commitment to protecting shared data.
- **Reduced risk of data breaches:** Minimizes the potential impact of security incidents.
- **Assured data integrity throughout the supply chain:** Ensures that data remains unaltered during transmission and storage.
- **Support for business continuity:** Protects critical information even in the event of a security breach.
- **Competitive advantage through enhanced security posture:** Differentiates the organization as a secure and reliable supply chain partner.
- **Minimized financial and reputational damage from potential breaches:** Reduces the costs and negative publicity associated with data leaks.
- **Facilitated secure data sharing across the supply chain:** Enables confidential information exchange with reduced risk.



4

Effective Log Management

Centralized real-time log collection is necessary for visibility.

Inputs

Log sources

Log Retention Policies

Log analysis techniques

Output

Centralized log management system with real time alerts

Effective log management involves the systematic collection, storage, and analysis of log data from various systems and applications across the supply chain, crucial for detecting anomalies, investigating incidents, and ensuring compliance with security policies

Recommended Actions:

- **Centralize log collection from all relevant systems:** Aggregate logs from various sources into a central repository for comprehensive analysis.
- **Utilize a Security Information and Event Management (SIEM) system:** Implement SIEM tools to correlate and analyze log data for threat detection.
- **Regularly backup logs to prevent data loss:** Create and maintain secure backups of log data to ensure long-term availability.
- **Define clear log retention policies:** Establish guidelines for how long different types of logs should be retained.
- **Conduct regular log audits:** Periodically review logs to ensure they are being collected and stored correctly.
- **Implement automated log analysis tools:** Use AI and machine learning algorithms to identify patterns and anomalies in log data.
- **Establish log review procedures and responsibilities:** Define roles and processes for regular log review and incident response.
- **Implement log integrity measures:** Use cryptographic hashing or similar techniques to ensure log data hasn't been tampered with.

Outcomes

A log management system provides visibility into supply chain activities.

- **Enhanced threat detection capabilities:** Quickly identify potential security incidents through log analysis.
- **Improved incident response times:** Enables faster investigation and resolution of security events.
- **Ensured regulatory compliance:** Meets legal and industry requirements for log management and retention.
- **Valuable operational insights:** Provides data for optimizing system performance and security measures.
- **Reduced system downtime:** Enables proactive identification and resolution of potential issues.
- **Assured data integrity and availability:** Maintains accurate and accessible records of system activities.
- **Support for a proactive security posture:** Allows for early detection and prevention of potential security threats.
- **Facilitated forensic investigations:** Provides crucial evidence for post-incident analysis and legal proceedings.
- **Enhanced system performance monitoring:** Offers insights into system behavior for optimization and troubleshooting.



5 Integrate Suppliers into Security

A single standard for both internal and external vendors.

Inputs

Supplier security requirements

Collaborative training program

Incident response plans

Output

Integrated supplier security framework

Integrating suppliers into security protocols involves establishing a collaborative approach to cybersecurity that includes all partners in the supply chain, ensuring consistent and comprehensive security measures across all entities involved.

Recommended Actions:

- **Develop a clear supplier security policy:** Create and communicate security standards and expectations for all suppliers.
- **Conduct regular security audits of suppliers:** Perform periodic assessments of suppliers' security practices and compliance.
- **Implement secure communication channels with suppliers:** Establish encrypted and authenticated methods for data exchange with suppliers.
- **Provide security training for suppliers:** Offer cybersecurity education and resources to enhance suppliers' security awareness.
- **Establish joint incident response plans:** Develop coordinated procedures for responding to security incidents across the supply chain.
- **Create a shared risk assessment framework:** Implement a common methodology for evaluating and managing supply chain risks.
- **Implement collaborative threat intelligence sharing:** Set up systems for real-time sharing of threat information among supply chain partners.
- **Develop supplier scorecards that include security metrics:** Create a system to evaluate and rank suppliers based on their security performance.

Outcomes

Suppliers are effectively integrated creating a unified approach to supply chain security:

- **Improved overall supply chain security posture:** Strengthens the entire supply network against cyber threats.
- **Reduced risk of data breaches across the supply network:** Minimizes vulnerabilities that could be exploited by attackers.
- **Improved trust and collaboration with suppliers:** Fosters stronger relationships based on shared security goals.
- **Compliance with industry standards and regulations:** Maintains adherence to legal and industry-specific security requirements.
- **Faster and more effective incident response:** Enables coordinated action to address security incidents quickly.
- **Increased supplier accountability for security:** Encourages suppliers to take an active role in maintaining security.
- **Cost savings through prevented security incidents:** Reduces financial losses associated with breaches and disruptions.
- **Unified approach to supply chain risk management:** Creates a consistent framework for addressing security challenges.



6

Comprehensive Risk Framework

Standard methodology to identify and address identified risks.

Inputs

Risk Assessment

Industry risk factors and trends

Risk mitigation strategies

Output

Integrated supplier security framework

Adopting a comprehensive risk management framework involves implementing a holistic approach to identify, assess, and mitigate risks, crucial for enhancing resilience and ensuring the stability of supply chain operations.

Recommended Actions:

- **Conduct regular risk identification and assessment:** Systematically identify and evaluate potential risks to the supply chain.
- **Develop and test various risk scenarios:** Create and simulate different risk events to prepare for potential disruptions.
- **Optimize supply chain processes for resilience:** Redesign processes to be more adaptable and resistant to disruptions.
- **Perform ongoing geopolitical analysis:** Monitor global events that could impact the supply chain and adjust strategies accordingly.
- **Foster partnerships for shared risk management:** Collaborate with suppliers and partners to distribute and mitigate risks.
- **Integrate advanced technologies for risk monitoring:** Utilize AI, IoT, and blockchain for real-time risk tracking and management.
- **Conduct regular risk management training for employees:** Educate staff on risk identification, assessment, and mitigation techniques.
- **Implement a risk-aware culture across the organization:** Encourage all employees to consider and report potential risks in their daily activities

Outcomes

Risk Management framework enabled proactive identification, assessment, and mitigation of risks

- **Enhanced supply chain resilience:** Improves the ability to withstand and recover from disruptions.
- **Proactive risk mitigation:** Addresses potential issues before they escalate into major problems.
- **Improved operational efficiency:** Streamlines processes by identifying and eliminating vulnerabilities.
- **Informed strategic decision-making:** Provides data-driven insights for long-term planning and strategy.
- **Competitive advantage through reliability:** Differentiates the organization as a dependable supply chain partner.
- **Ensured regulatory compliance:** Meets legal and industry requirements for risk management.
- **Increased stakeholder confidence:** Demonstrates a proactive approach to managing supply chain risks.
- **Improved long-term sustainability of the supply chain:** Ensures the supply chain can adapt and thrive in changing environments.
- **Enhanced ability to seize opportunities:** Enables quick response to positive market changes and new prospects.



Implementing continuous monitoring and assessment involves the ongoing evaluation of security measures and practices to ensure the integrity, confidentiality, and availability of supply chain operations, helping to identify vulnerabilities, detect threats, and ensure compliance with security standards.

Recommended Actions:

- **Establish a security baseline for normal operations:** Define standard operating parameters to detect deviations quickly.
- **Deploy advanced real-time monitoring tools:** Implement technologies for continuous surveillance of supply chain activities.
- **Conduct regular security audits and assessments:** Perform periodic in-depth evaluations of security measures and practices.
- **Integrate threat intelligence feeds:** Incorporate up-to-date information on emerging threats and vulnerabilities.
- **Implement automated alert and response systems:** Set up systems to automatically detect and respond to potential security incidents.
- **Develop key performance indicators (KPIs) for security:** Establish metrics to measure and track security performance over time.
- **Establish a continuous improvement process for security measures:** Regularly review and update security practices based on monitoring results.
- **Implement predictive analytics for proactive risk management:** Use data analysis to forecast potential security issues before they occur.

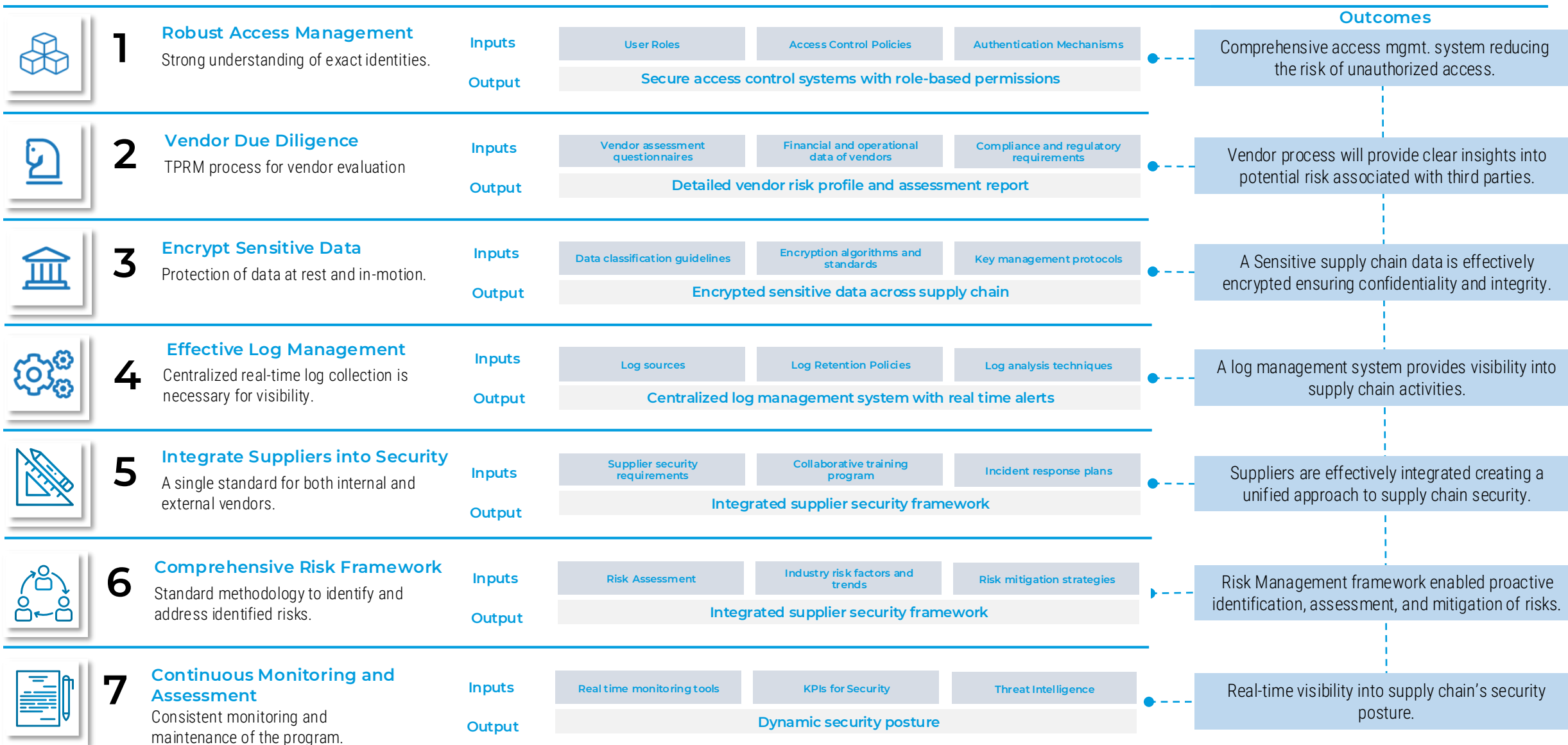
Outcomes

Real-time visibility into supply chain's security posture.

- **Enhanced early threat detection capabilities:** Identifies potential security issues in their initial stages.
- **Improved compliance with evolving security standards:** Ensures ongoing adherence to changing regulatory requirements.
- **Increased operational resilience:** Enhances the ability to maintain operations during security incidents.
- **Proactive risk management:** Addresses potential threats before they can cause significant damage.
- **Cost efficiency through early issue resolution:** Reduces expenses associated with major security incidents.
- **Ensured data integrity and confidentiality:** Maintains the trustworthiness and privacy of supply chain information.
- **Improved stakeholder confidence:** Demonstrates a commitment to ongoing security and risk management.
- **Adaptability to emerging security challenges:** Enables quick responses to new types of threats and vulnerabilities.
- **Enhanced supply chain visibility:** Provides real-time insights into the security status of the entire supply network.

Plan for Addressing Supply Chain Security

Electronic Supply Chain- the following seven steps will help reduce risk to the organization.



Call to Action



©2025 CyberOne LLC. All rights reserved.

Trends for the Future

1. Increased use of AI and predictive analytics for risk prediction and optimization
2. Enhanced supply chain visibility through real-time tracking and monitoring tools
3. Greater focus on sustainability and ESG goals (environmental, social, and governance)
4. Regional diversification of supplier hubs to mitigate geopolitical risks
5. Adoption of emerging technologies like IoT and blockchain for improved risk management
6. Shift towards proactive, data-driven risk management strategies



Taking Action

Supply Chain Security is Hard

- No easy button or single product to purchase
- Extend your security controls to suppliers for a single approach
- Seek out help!
- Remain innovative



**Don't miss CISO-XC on
Wednesday**

<https://www.cisoxc.com/event-details/ciso-xc-atx-request-for-rsvp>



©2025 CyberOne LLC. All rights reserved.



AUSTIN INAUGURAL

FEBRUARY 26, 2025 | AUSTIN, TEXAS

LINK BELOW

[WWW.CISOXC.COM](https://www.cisoxc.com)

