We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Securing the Unseen: Safeguarding Against Hidden Supply Chain Threats

November 2024

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Presentation Overview

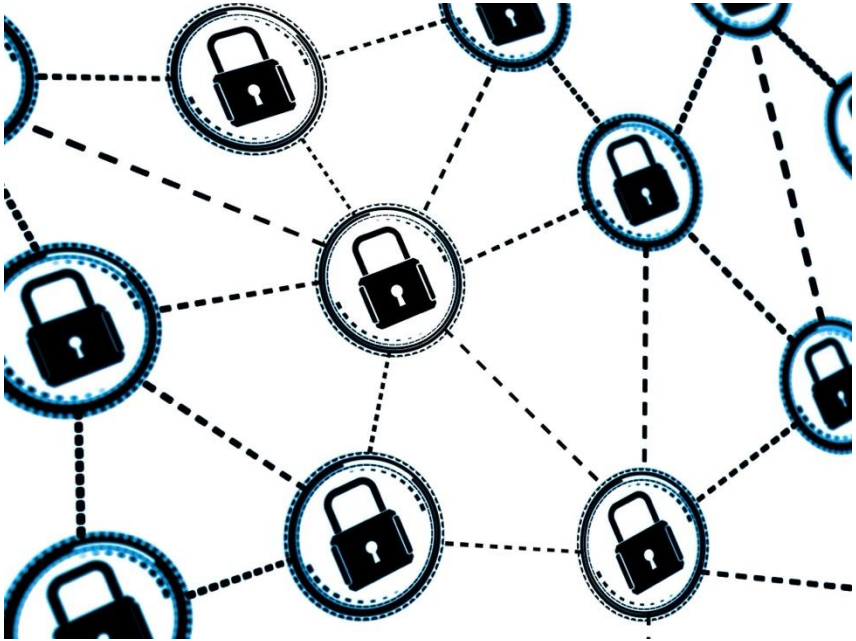
Cyber Supply Chain Risk Management

Specific Risks Faced by Financial Institutions

Best Practices for Mitigating Risks

Implementing a Cyber Supply Chain Risk Management Program

What is Cyber Supply Chain Risk?



What is Cyber Supply Chain Risk?

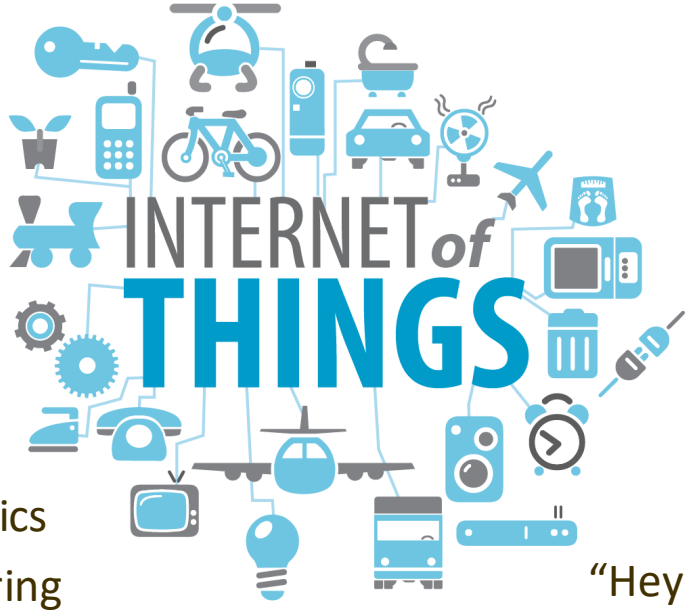
It is the risk that an organization's information and technology systems and data may be compromised as a result of vulnerabilities and threats in the supply chain.

Vulnerabilities and Threats in the Supply Chain

Cyber supply chain risk arises due to vulnerabilities and threats in the supply chain which can be exploited by attackers to compromise an organization's information and technology systems and data.

Raise Your Hand if You Work for a Tech Company

- Security Cameras
- Motion Sensors
- Logistics/GPS Tracking
- Print Vendors
- Smart TV Displays
- HVAC
- Digital Assistance
- Cloud Applications & Analytics
- Bio-Medical Care & Monitoring
- Core Data Processing
- Hosted Application Processing



Security cameras

Garage door

Home thermostat

Cable TV remote

Smart TV

Sleep number bed

Roomba

Apple Watch or FitBit

“Hey Siri, what’s my balance?”

Why is Cyber Supply Chain Risk Important?

Interruption of Operations

Data Breaches

Intellectual Property Theft

Security Incidents

Real-world Cyber Supply Chain Risk Incidents Over the Past 5 Years

SolarWinds Attack (2020)

Capital One Breach (2023)

American Express Third-Party Breach (2021)

Bank of America (2023)

Open-Source Software Attack (2023)

Recent Incidents Impacting Financial Institutions

- Ongoing Operations Outage (2021)
- Trellance Ransomware Attack (2023)
- MOVEit Vulnerability (2023)

Are we at the Tipping Point?

AMERICAN BANKER

TECHNOLOGY

Tech issues afflict banks, Microsoft after critical CrowdStrike glitch

By Carter Pape, Miriam Cross July 19, 2024, 12:44 p.m. EDT 10 Min Read

CrowdStrike outage sparks global chaos with airline, bank and other disruptions

Microsoft Windows computers were affected b
the outage.

By Sam Sweeney and Jon Haworth
July 18, 2024, 11:41 PM

Reddit

MARKETPLACE
Search For & Place Classifieds

Austin American-Statesman
SERVING OUR COMMUNITY SINCE 1871

News Sports Hookem.com Austin360 Opinion Advertise Obituaries eNewspaper Legals

The Microsoft outage also impacted banks around the world. Banks in Australia, South Africa, New Zealand and Britain experienced interruptions in services, according to CNN.

According to monitoring app Downdetector, the following banks have been affected by the Crowdstrike outages:

- Arvest Bank
- Bank of America
- Capital One
- Charles Schwab
- Chase
- TD Bank
- US Bank
- Wells Fargo

What is Cyber Supply Chain Risk Management?

Cyber supply chain risk management refers to the process of identifying and mitigating risks related to third-party suppliers that provide critical goods and services to financial institutions.

This process includes risk assessments, due diligence, and ongoing monitoring of suppliers.

Why is Cyber Supply Chain Risk Management Important for Financial Institutions?

Critical Role of Financial Institutions

Cyber supply chain risk management is essential to maintain trust and confidence in the financial system.

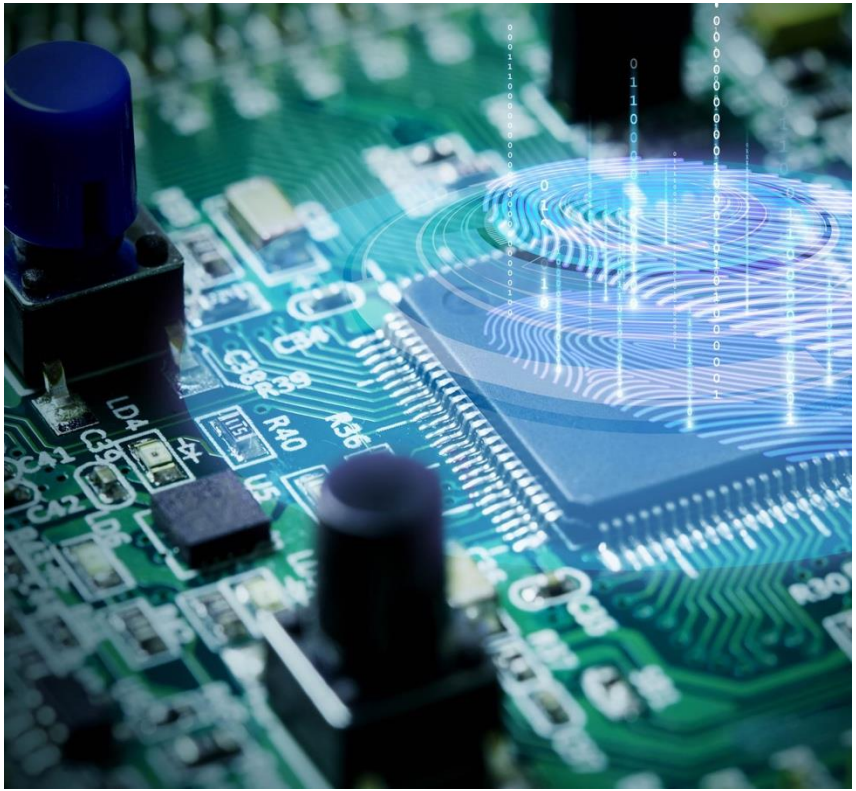
Third-Party Suppliers

Financial institutions rely on third-party suppliers to provide critical goods and services, such as payment processing and data storage.

Consequences of Breach

A breach in the supply chain can have severe consequences for the financial institution's operations, reputation, and customers.

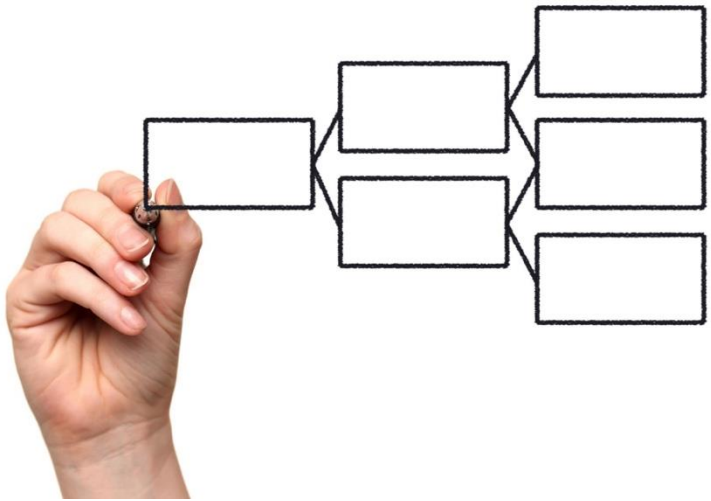
Identifying and Assessing Cyber Supply Chain Risk



Think in terms of ”classic risk assessment…”

- Identify assets
- Identify threats
- Evaluate likelihood
- Evaluate impact

Supply Chain Mapping

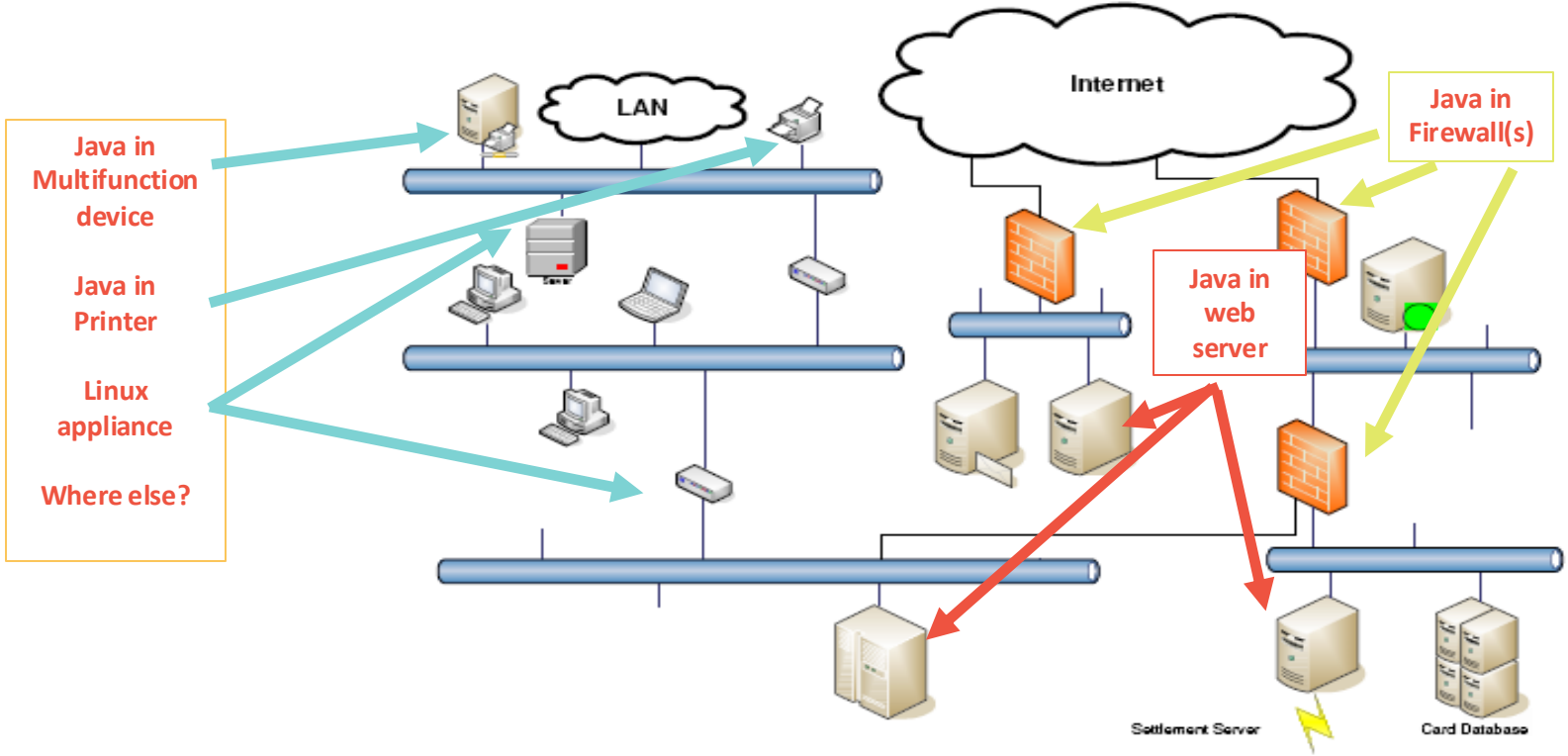


Supply chain mapping is the process of identifying and assessing all of the suppliers and vendors that provide critical products and services to an organization. This can help to identify potential vulnerabilities and threats in the supply chain.

Threat Assessment

Threat assessment involves identifying potential risks to the supply chain, including natural disasters, cyberattacks, and human error.

Example: Java Software and Log4j



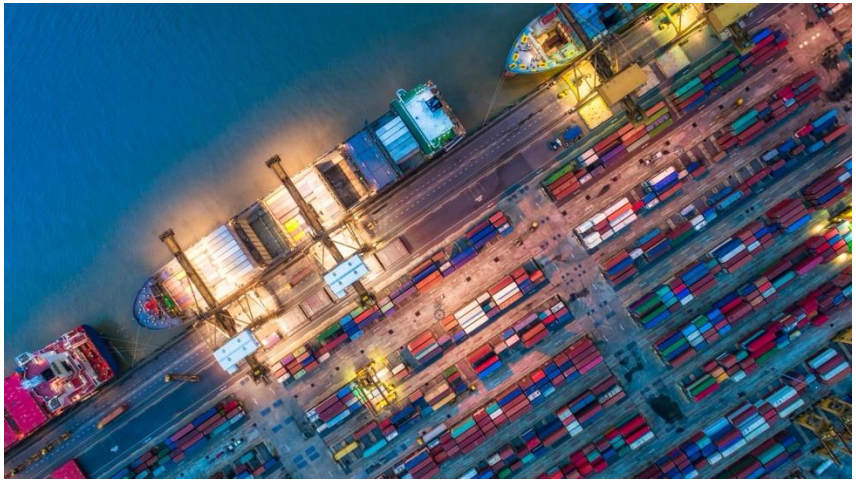
Software Vendor/Supply Chain Risk Management

- All software products have bugs/vulnerabilities
  - Key questions:
    - Do we have accurate system and data inventory?
    - What does this software application have access to?
    - What user account/privileges are given to it?
    - What do we need to do for our due diligence?
    - What impact does this software have on the institution…
      - If it is hacked/breached?
      - If it is down for… 2 hours? 2 days? 2 weeks? 2 months?

Pick your hosted software vendor:

1. CrowdStrike
2. Trellance
3. MoveIT
4. Kronos
5. Solarwinds
6. MS Exchange
7. _____

Supplier Categorization and Risk Prioritization



Strategic Suppliers: Long-term partners critical to business operations.

Tactical Suppliers: Essential but replaceable suppliers.

Niche Suppliers: Providers of unique products/services, harder to replace.

Commodity Suppliers: Readily available suppliers with low switching costs.

Best Practices for Mitigating Risks

Establish Clear Security Requirements for Suppliers

Financial institutions should establish clear security requirements for suppliers to ensure they have adequate security measures in place.

Conduct Regular Security Assessments

Financial institutions should conduct regular security assessments of their suppliers to ensure compliance with security requirements and identify any potential vulnerabilities.

Best Practices for Mitigating Risks

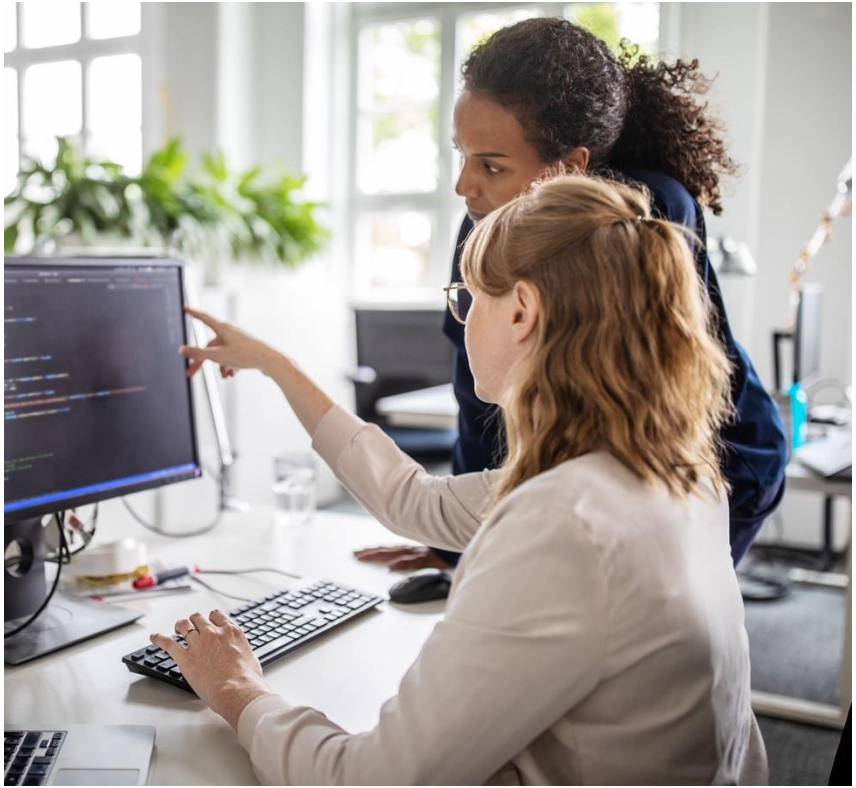
Monitor Supplier Compliance

Financial institutions should monitor supplier compliance with security requirements and take corrective action if necessary to mitigate any potential security risks.

Have a Plan to Respond to Security Incidents and Breaches

Financial institutions should have a plan in place to respond to security incidents and breaches, including procedures for reporting and investigating incidents.

How to Implement Cyber Supply Chain Risk Management



Establish Clear Policies and Procedures

Establishing clear policies and procedures for cyber supply chain risk management is essential to ensure that all stakeholders understand their roles and responsibilities in implementing an effective risk management program.

Designate a Person or Team Responsible for Managing Supply Chain Risks

Designating a person or team responsible for managing cyber supply chain risks helps to ensure that all risks are identified, assessed, and managed in a timely and effective manner.

Policies and Procedures

Risk Assessment

Establishing a risk assessment process is necessary to identify potential cyber supply chain risks. This includes assessing the security posture of suppliers to ensure they are meeting security standards and requirements.

Due Diligence Processes

Conducting due diligence on suppliers is necessary to verify their security posture and ensure they are not engaged in any malicious activities. This includes conducting background checks and verifying their security policies and procedures.

Security Requirements for Suppliers

Banks should establish security requirements for suppliers to ensure that they are meeting the same security standards as the bank. This includes implementing appropriate security controls and monitoring for compliance.

Incident Response Plans

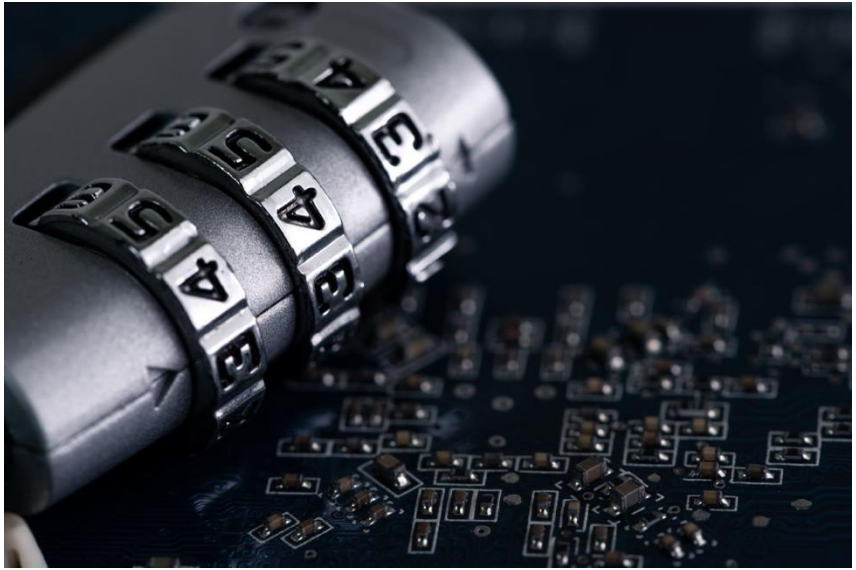
Financial institutions should have an incident response plan in place to effectively respond to a cyber supply chain attack. The plan should include roles and responsibilities, communication protocols, and procedures for mitigating the attack.

Supply Chain Risk Management Team

Designating a person or a team responsible for managing supply chain risks is essential to ensure that the program is properly implemented and maintained.

They should have the authority and resources necessary to carry out risk assessments, due diligence, and ongoing monitoring of suppliers.

Conclusion



Cyber supply chain risk management is essential for FIs to protect themselves from cyber threats and ensure the security of their supply chains. By implementing best practices and establishing clear policies and procedures, FIs can mitigate the risks associated with their suppliers and ensure the continuity of their operations.

To Learn more about Cybersecurity Supply Chain Risk Management:

Randy Romes, CISSP, CRISC, CISA, MCP, PCI-QSA
Email: randy.romes@claconnect.com
Mobile: 612.397.3114

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS

C-SCRM Resources

NIST 800-161r1 – Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations:

Cybersecurity Supply Chain Risk Management (C-SCRM) is a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures. The purpose of this publication is to provide guidance to enterprises on how to identify, assess, select, and implement risk management processes and mitigating controls across the enterprise to help manage cybersecurity risks throughout the supply chain.

NIST Cyber Security Framework 2.0:

Building on previous version CSF 2.0 contains new features that highlight the importance of governance and supply chains.

ISACA Journal Vol 6 – The Anatomy of Information and Communications Technology (ICT) and Services Supply Chain Risk Management:

The ICT and services supply chain is the entire chain of activities connecting the life cycle of procurement and maintenance of ICT systems and services. More specifically, the ICT supply chain is an ecosystem that covers the entire life cycle of ICT hardware and software provided by third-party vendors, suppliers, system integrators and contractors and a wide range of managed services by various providers.

ISACA Avoiding the Supply Chain Domino Effect:

Global supply chains are increasingly complex and interconnected. Failure to identify and prepare an effective supply chain risk management plan can have dire consequences for an organization’s revenue, costs, brand reputation and shareholder value.

CISA and National Risk Management Center:

ICT Supply Chain Risk Management, governance, and associated risk domains.