



Supply Chain Risk Management

16th September 2014

Topics

- Background
- Approach
- Status



Background

e-Governance in India

- National e-Governance Plan 2006
- 31 Mission Mode Projects
- Quality Assurance in e-Governance

Quality Assessment of e-Governance Solutions

What is required – A Formal Approach

Quality solutions requires context specific Processes should be in place

For Quality Assessment of these solutions we need :

- Quality Model for e-Governance solution
- Evaluation Model for e-Governance solution

Quality Model

Quality characteristics of an IT system can be defined in terms of Functionality, Performance, Reliability, Usability, Security, and Portability. These quality characteristics can be defined by using Product standards, achieved by following Management and Technical process and Verified and Validated by different techniques such as inspections/Reviews/Testing etc.) of both product and processes.

Quality Characteristics	Defined	Achieved by following	
		Software Process	System Process
Functionality	ISO 9126 / ISO/IEC 25010:2011	ISO/IEC 12207	ISO/IEC 15288
Performance	ISO 9126 / ISO/IEC 25010:2011	ISO/IEC 12207	ISO/IEC 20000-1
Reliability	ISO 9126 / ISO/IEC 25010:2011	ISO/IEC 12207	ISO/IEC 20000-1
		IEEE982.1	
Usability	ISO 9241	ISO/IEC 13407	ISO 9241
Security	ISO 9126 / ISO/IEC 25010:2011 ISO/IEC 27034 ISO/IEC 27033	ISO/IEC 21827	ISO/IEC 27001
Portability	ISO 9126 / ISO/IEC 25010:2011	ISO/IEC 12207	ISO/IEC 15288
Maintainability	ISO 9126 / ISO/IEC 25010:2011	ISO/IEC 14764:2006	ISO/IEC 15288

Evaluation Model

Architecture Layer	System/Component of Interest		Quality Requirements
User Layer	Citizen/Business/ Government		Apex Gate User Satisfaction
Service Access Layer	Websites	Mobile Devices	Quality Gates (Essential) <ol style="list-style-type: none"> 1. Organizational Process 2. Software Application Quality 3. Information Security 4. IT Service Management
	Biometrics	Smart Cards	
Technology Layer	Data Centre	Wide Area Network	
	Common Service Centre	Service Delivery Gateway	
Organisational Layer	Government Department		



APPROARCH

Supply Chain Risk Management

Problem Statement

- Information and Communication Technology (ICT) products are assembled, built, and transported by multiple vendors around the world before they are acquired ***without the knowledge of the acquirer***
- Challenges range from poor acquirer practices to lack of transparency into the supply chain
 - **Substantial number of organizations or people can “touch” an ICT product without being identified**
 - No standardized methodology or lexicon exists for managing ICT supply chain risks
 - Poor ICT products and services acquisition practices contribute to acquirers’ lack of understanding what is in their supply chain
 - Counterfeit hardware and software proliferate
 - Acquirers do not have a framework to help enforce security and assurance compliance for vendors

Supply Chain: PERSPECTIVES

- IT and Communications products are assembled, built, and transported by multiple vendors around the world.
- Software contributions include reusable libraries, custom code, commercial products, open source

Supply Chain SECURITY

- Nodes of storage & throughput
- Lines of transport (& communication)

Supply Chain RESILIENCE

- Multi-sources
- Multi-nodes
- Multi-routes

Product INTEGRITY

How do we improve our trust & confidence in HW, SW & Services we source from a global supply chain?

Supply Chain Risk Management

APPROARCH

- Ensure SCRM is a part of RFP/Contract document
- Use essential security and foundation practices
- Use ISO 27001 (ISMS) Framework (focus on ISO 27002)
- Leverage Support Standard (ISO/IEC 27036)
- Use Guidance from NIST 800-161

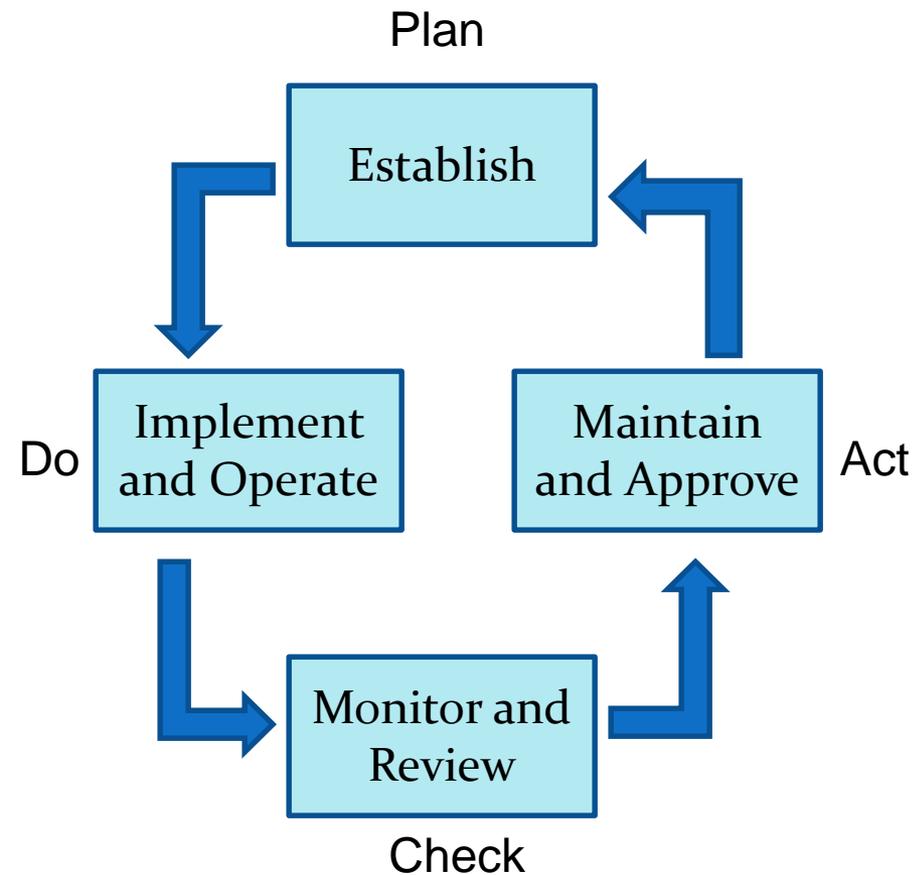
Essential Security and Foundational Practices

- **Management Systems:** ISO 9001 - Quality, ISO 27001 – Information Security, ISO 20000 – IT Service Management, ISO 28000 – Supply Chain Resiliency
- **Security Controls:** ISO/IEC 27002, NIST 800-53, NIST 800-161
- **Lifecycle Processes:** ISO/IEEE 15288 - Systems, ISO/IEEE 12207 – Software
- **Risk Management:** ISO 31000 - overall, ISO/IEC 27005 - security, and ISO/IEC 16085 - systems
- **Industry Best Practices:** CMMI, Assurance Process Reference Model, COBIT, ITIL, PMBOK, eSCM

e-Gov Security Assurance Framework based on ISO 27001

Why Use ISO/IEC 27001?

- **Integrate security governance into business and IT processes**
 - Standardizes security processes and controls
 - Establish a common approach to risk management
 - Reduce the likelihood, severity, duration and cost of incidents
- **Establish risk-based control selections as a standard for risk management**
 - Focus resources only on your organization's risks
 - Facilitate identification and elimination of non critical data
 - Ensure costs reflect the risk's appetite
- **Use ISMS processes to improve overall assets management capabilities**
 - Identify and eliminate redundant, duplicate and obsolete assets
 - Enable simplified cost determination of new or revised control deployments
 - Provide risk reference point for both operations and management



Using ISO/IEC 27036 with other SC27 Standards

Certify against ISMS and...

ISO/IEC 27001 –
Information Security
Management Systems

...general requirements for
supplier relationships

ISO/IEC 27036-2 –
Information Security for
Supplier Relationships -
Requirements

...ICT SCRM Guidance

ISO/IEC 27036- ICT Supply –
Information Security for
Supplier Relationships- ICT
Supply Chain Security

...Cloud-specific Guidance

ISO/IEC 27036-4-
Information Security for
Supplier Relationships –
Cloud

...27002 Controls

ISO/IEC 27002 – Code of
Practice for Information
Security Controls

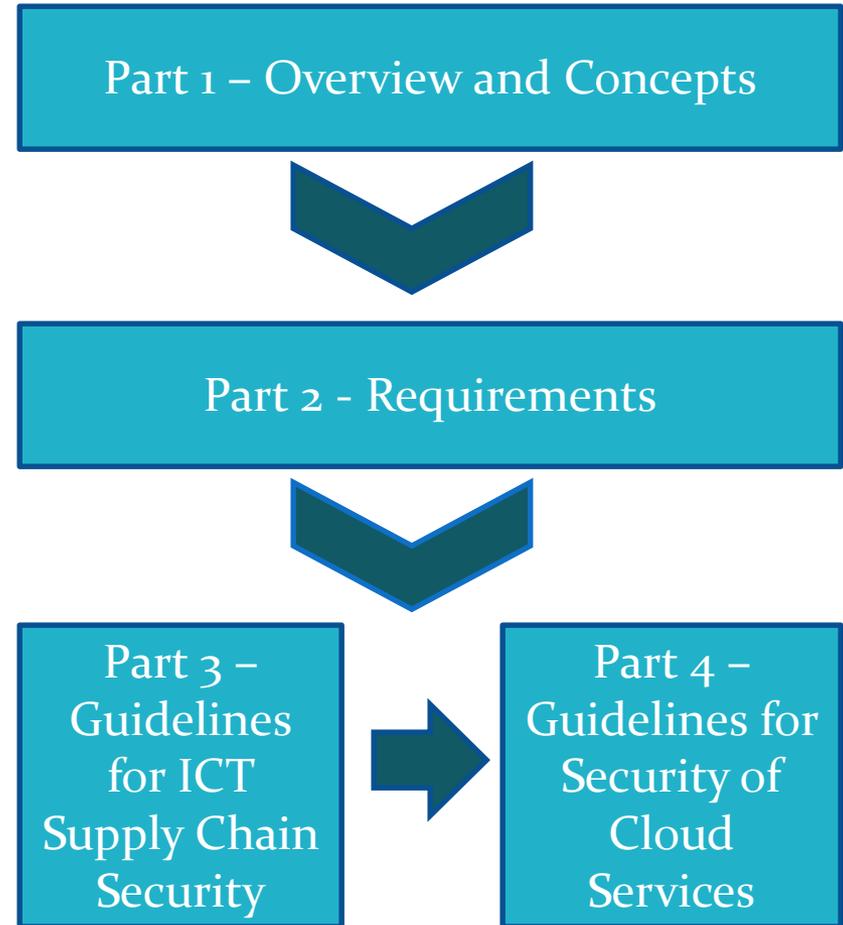
...27017 Cloud Controls

ISO/IEC 27017 – ISMS –
Code of Practice for
information security
controls for cloud
computing services



ISO/IEC 27036, Information Technology – Security Techniques – Information Security for Supplier Relationships

- Addresses Acquirer and Supplier Practices
- Applies to all types of organizations e.g., commercial, public sector, non-profit and all types of supplier relationships that may have security implications
- Harmonized with ISO standards for system/software engineering and information security
- Part 1-3 are currently Draft International Standard; Part 4 is Working Draft



ISO/IEC 27036 Information Security Management System (ISMS) Family of Standards

Governance

Terminology

Requirements

Guidelines

ISO/IEC 27000 – Overview and Vocabulary

ISO/IEC 27001 – ISMS Requirements

ISO/IEC 27006 – Audit and Certification Requirements

ISO/IEC 27002 - Code of Practice

ISO/IEC 27003 – ISMS Guidelines

ISO/IEC 27007 – Audit Guidelines

ISO/IEC 27008 – Guidance for auditors on ISMS controls

ISO/IEC 27004 - Measurement

ISO/IEC 27005 – Risk Management

ISO/IEC 270XX (concept) – Sector-Specific Guidelines

ISO/IEC 27017(concept)- ISO/IEC 27017-ISMS- Code of Practice for information security controls for cloud computing services

Security Engineering

Tamper Protection Study Period

ISO/IEC 21913 – Secure System Engineering Principles & Techniques

ISO/IEC 15408- Common Criteria

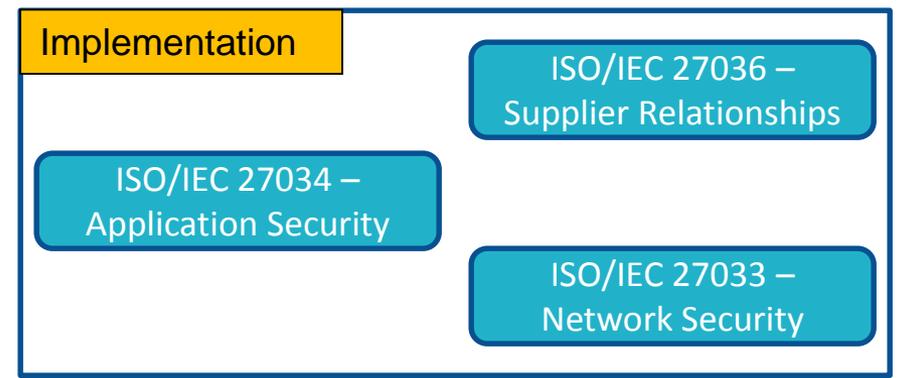
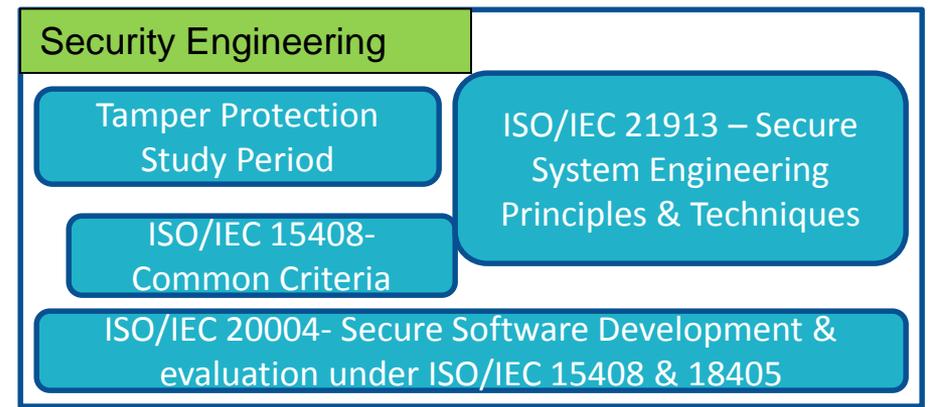
ISO/IEC 20004- Secure Software Development & evaluation under ISO/IEC 15408 & 18405

Implementation

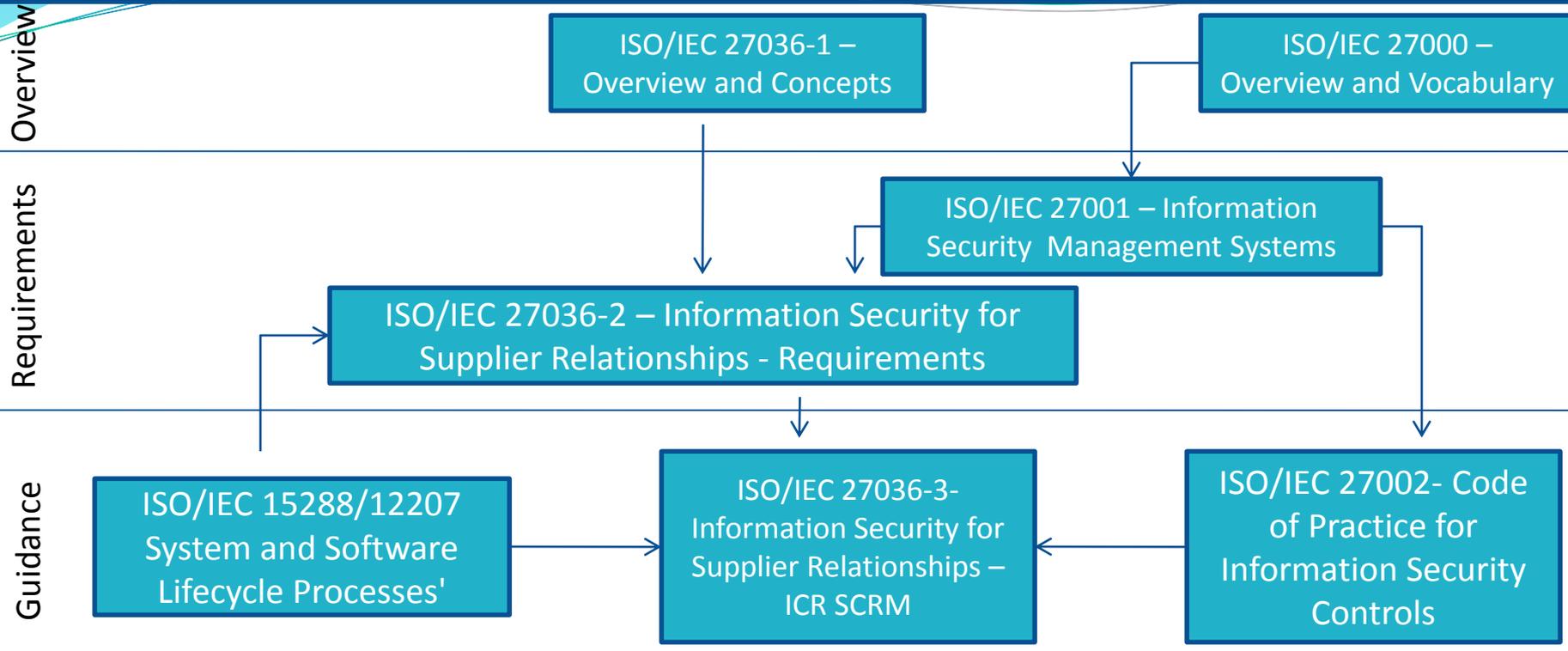
ISO/IEC 27036 – Supplier Relationships

ISO/IEC 27034 – Application Security

ISO/IEC 27033 – Network Security



ISO/IEC 27036 Dependencies and Influences



- Processes & Techniques
- ISO/IEC 15026-Software Assurance
 - ISO/IEC 27034-Application Security
 - Security Engineering and Design Techniques
 - NASPO & other Anti-counterfeiting techniques
 - Microsoft Secure Development Lifecycle (SDL)
 - SAFECode
 - OWASP
 - BSIMM

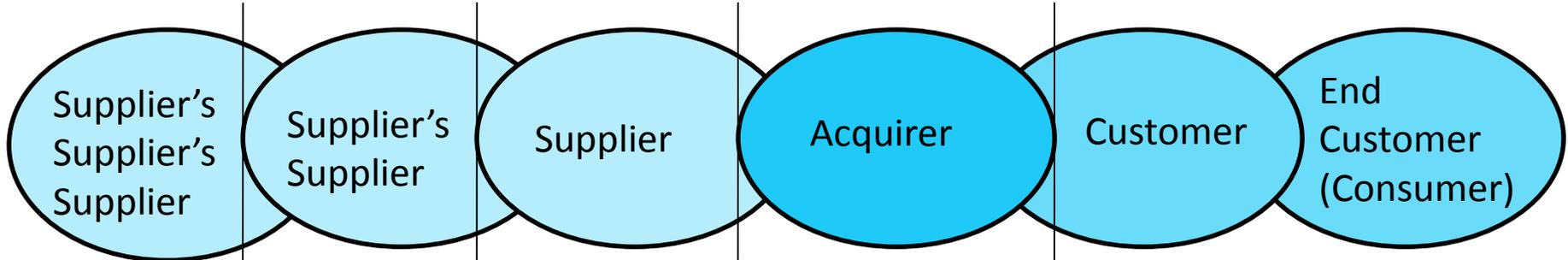
- Common Criteria – ISO/IEC 15408
- OMG KDM BPMN , RIF, XMI, RDF
- OWASP Top 10
- SANS TOP 25
- Secure Content Automation Protocol (SCAP)
- Secure Coding Checklists
- Encryption
- Software Asset Tagging
- Trusted Platform Module (TPM)



Status

Experience

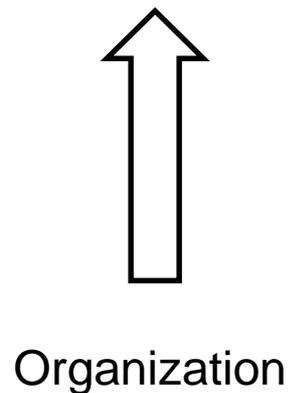
Registered Devices (Biometric Devices–Finger Print Scanner)



.....

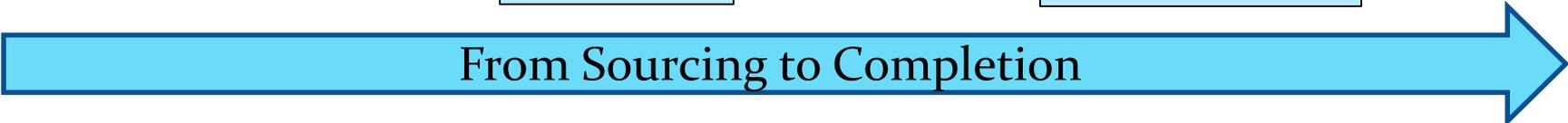
Tier 2

Tier 1



Upstream

Downstream



Key Concepts

Downstream : Handling processes and movements of products and services that occur after an entity in the supply chain takes custody of the products and responsibility for services.

Outsourcing : Acquisition of services (with or without products) in support of a business function for performing activities using supplier resources rather than acquirer's.

Supplier Relationship : Agreement(s) between acquirers and suppliers to conduct business, deliver products or services, and realize business benefits.

Supply Chain : Set of organizations with linked set of resources and processes, each of which act as an acquirer, supplier or both to form successive supplier relationship established upon placement of a purchase order, agreement or other formal sourcing agreement.

Visibility : Property of a system or process that enables system elements and processes to be documented and availability for monitoring and inspection.

Quality Assessment of Registered Devices

- For Services linked with financial domain it is desirable that each device is uniquely identified and secure while capturing and storing data in the device.
- Devices can be registered with Aadhaar system for Encryption Key Management.
- Aadhaar authentication server will be able individually identify and validate these devices and manage encryption keys on each registered device.
- STQC responsible for assessing quality of registered devices.
 - Framework uses quality system, ISMS (ISO 27001 and 27002) and other family standards framework which includes ISO 13491 standards on Banking – Secure Cryptographic devices.
 - Assurance is achieved by implementing processes, contract agreements throughout supply chains and evidence of conformities.

Lifecycle Approach

Agreement Processes

Acquisition Process

Supply Process

Organization Project-enabling Processes

Life Cycle Model Management Process

Infrastructure Management Process

Project Portfolio Management Process

Human Resource Management Process

Quality Management Process

Project Processes

Project Planning Process

Project assessment & Control Process

Decision Management Process

Risk Management Process

Configuration Management Process

Information Management Process

Measurement Process

Technical Processes

Architectural Design Process



Supplier Relationship Planning Process

Supplier Selection Process

Supplier Relationship Agreement Process

Supplier Relationship Management Process

Supplier Relationship Termination Process

Scope

Fundamental and high-level information security requirement for acquirers and suppliers scheme commonly applicable to instances of supplier relationships

Fundamental information security requirement for acquirers and when establishing and maintaining an instance of supplier relationships

Essential ICT supply chain security practices

- a) **Chain of custody:** the acquirer and supplier have the confidence that each change and handoff made during the element's lifetime is authorized, transparent and verifiable;
- b) **Least privilege access:** personnel can access critical information and information systems with only the privileges needed to do their jobs;
- c) **Separation of duties:** control the process of creation, modification, or deletion of data or the process of development, operation, or removal of hardware and software by ensuring that no one person or role alone can complete a task;
- d) **Tamper resistance and evidence:** attempts to tamper are obstructed, and when they occur they are evident and reversible;
- e) **Persistent protection:** critical data and information are protected in ways that remain effective even if the data or information are transferred from the location where it was created or modified;
- f) **Compliance management:** the success of the protections within the agreement can be continually and independently confirmed;
- g) **Code assessment and verification:** methods for code inspection are applied and suspicious code is detected;
- h) **ICT supply chain security training:** organization's ability to effectively train relevant personnel on information security practices. This should include secure development practices, recognition of tampering, etc., as appropriate;

- i) **Vulnerability assessment and response:** a formal understanding by acquirer of how well their suppliers are equipped with the capability to collect input on vulnerabilities from researchers, customers, or sources, and produce a meaningful impact analysis and appropriate remedies in the short timeframe involved. This should include acquirer and supplier agreement on systematic repeatable vulnerability response processes;
- j) **Defined expectations:** clear language regarding the requirements to be met by the element and design/development environment is set forth in the agreement. This should include commitment to provide information security testing, code fixes and warranties about the development, integration, and delivery processes used;
- k) **Ownership and responsibilities:** acquirer's and supplier's ownership of intellectual property rights and the other party's responsibilities for protecting the intellectual property rights are identified in the agreement;
- l) **Avoidance of gray-market components:** many ICT supply chain risks can be avoided by requiring verification of authenticity for system components;
- m) **Anonymous acquisition:** when appropriate and feasible, practice anonymous acquisition; when acquirer identity is sensitive, obscure the connection between the ICT supply chain and the acquirer;
- n) **All-at-once acquisition:** components for long-life systems (durable automatic controls) can become obsolete and increase ICT supply chain risk, acquiring all spare parts within a specified time-frame reduces these risks;
- o) **Recursive requirements for suppliers:** contracts can establish that suppliers place and validate ICT supply chain requirements on their upstream suppliers.



Thanks