Information security in supplier relationships: Frameworks

Andrey Prozorov, CISM, CIPP/E

11.05.2020

Most (if not all) organizations around the world, whatever their size or domains of activities, have ***relationships with suppliers*** *of different kinds that deliver products or services.*

Such ***suppliers*** *can have either a direct or indirect access to the information and information systems of the acquirer, or will provide elements (software, hardware, processes, or human resources) that will be involved in information processing. Acquirers can also have physical and/or logical access to the information of the supplier when they control or monitor production and delivery processes of the supplier.*

Thus, ***acquirers and suppliers can cause information security risks to each other****. These risks need to be assessed and treated by both acquirer and supplier organizations through appropriate management of information security and the implementation of relevant controls.*

By ISO 27036

Key terms (by ISO 27036)[1]

Acquirer - stakeholder that procures a product or service from another party.

Note 1 to entry: Procurement may or may not involve the exchange of monetary funds.

Acquisition - process for obtaining a product or service.

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

Key terms (by ISO 27036, NIST and COBIT)$_2$

Supplier - organization or an individual that enters into agreement with the acquirer for the supply of a product or service.

Note 1 to entry: Other terms commonly used for supplier are **Contractor**, **Producer**, **Seller**, or **Vendor**.

Note 2 to entry: The acquirer and the supplier can be part of the same organization.

Note 3 to entry: Types of suppliers include those organizations that permit agreement negotiation with an acquirer and those that do not permit negotiation with agreements, e.g. end-user license agreements, terms of use, or open source products copyright or intellectual property releases.

Supplier - Product and service providers used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products of services provided to that organization's Buyers.

Vendor - Enterprise that sells products or services to other enterprises.

Key terms (by ISO 27036)[3]

Supplier relationship - agreement or agreements between acquirers and suppliers to conduct business, deliver products or services, and realize business benefit.

Supply chain - set of organizations with linked set of resources and processes, each of which acts as an acquirer, supplier, or both to form successive supplier relationships established upon placement of a purchase order, agreement, or other formal sourcing agreement.

Note 1 to entry: A supply chain can include vendors, manufacturing facilities, logistics providers, distribution centres, distributors, wholesalers, and other organizations involved in the manufacturing, processing, design and development, and handling and delivery of the products, or service providers involved in the operation, management, and delivery of the services.

Note 2 to entry: The supply chain view is relative to the position of the acquirer.

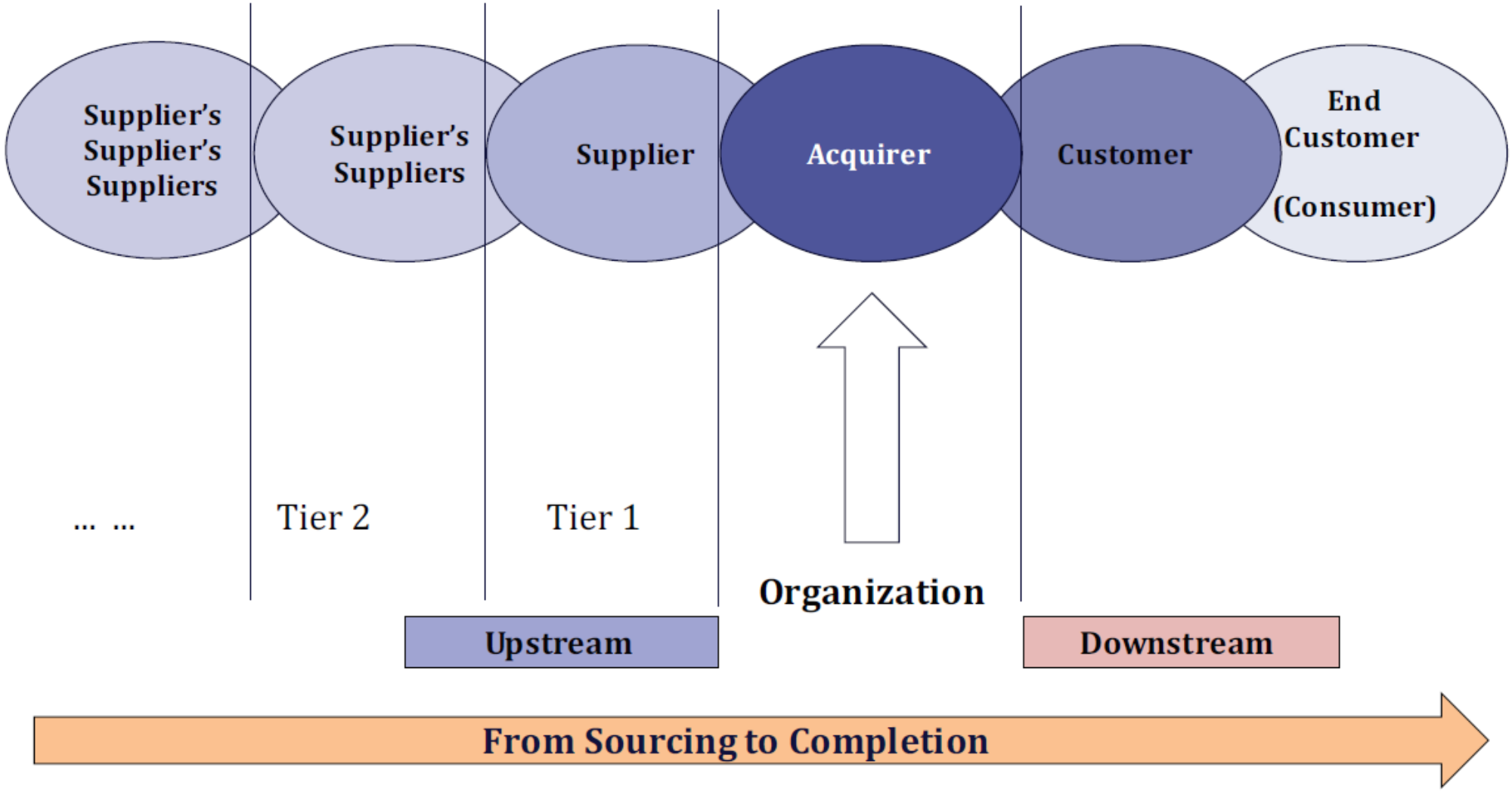


Figure 1 — Supply Chain Relationships

By ISO 27036

Major Frameworks

Supply Chain Management is a important part of the ISMS:

- ISO 27001 / ISO 27002 (A.15 Supplier relationships)
- The ISF Standard of Good Practice for Information Security (SC. Supply Chain Management)
- NIST Cybersecurity Framework (ID.SC Supply Chain Risk Management)
- NIST SP 800-53 Rev. 4 (SA-12 Supply Chain Protection)

ISO 27001. A.15 Supplier relationships

15.1 Information security in supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

A.15.1.1 Information security policy for supplier relationships

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

A.15.1.2 Addressing security within supplier agreements

All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

A.15.1.3 Information and communication technology supply chain

Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

A.15.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

A.15.2.1 Monitoring and review of supplier services

Organizations shall regularly monitor, review and audit supplier service delivery.

A.15.2.2 Managing changes to supplier services

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved of risks.

ISF SoGP SC. Supply Chain Management

SC1 External Supplier Management

SC1.1 Supplier Management Framework

Principle A security management framework should be established that includes appropriate external supplier security steering groups, policies, processes, registers and information risk assessments and security arrangements.

Objective To ensure information risks are identified and managed effectively throughout all stages of the relationship with external suppliers (including organisations in the supply chain).

SC1.2 Supplier Procurement

Principle A process should be established to integrate security into the procurement of products and services from external suppliers.

Objective To provide assurance that security requirements are addressed effectively when products or services are delivered by external suppliers.

SC1.3 Supplier Contracts

Principle The use of products and services provided by external suppliers should be supported by contracts that include appropriate security requirements.

Objective To define security requirements for products and services provided by external suppliers and specify how they will be met.

SC2 Cloud Services

SC2.1 Cloud Security Management

Principle A comprehensive, documented security management approach for the acquisition and use of cloud services should be developed and communicated to all individuals who may purchase, develop, configure or use cloud services.

Objective To ensure all necessary security arrangements are implemented for the use of cloud services, and that information risks are managed in cloud environments.

SC2.2 Core Cloud Security Controls

Principle A set of fundamental cloud security controls should be created and implemented effectively, tailored to the needs of the organisation, that cover a broad range of the most common cloud security issues.

Objective To address weak or insufficient cloud security controls and help the organisation use cloud services securely in a heterogeneous, multi-cloud environment.

NIST CSF. Supply Chain Risk Management (ID.SC)

Cyber **SCRM** activities may include:

- Determining cybersecurity requirements for suppliers
- Enacting cybersecurity requirements through formal agreement (e.g., contracts)
- Communicating to suppliers how those cybersecurity requirements will be verified and validated
- Verifying that cybersecurity requirements are met through a variety of assessment methodologies, and
- Governing and managing the above activities

ID.SC The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.

ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.

ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.

ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.

ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.

Special guides

- ISO 27036 Securing supplier relationshiips
  - Part 1: Overview and concepts
  - Part 2: Requirements
  - Part 3: Guidelines for ICT supply chain security
  - Part 4: Guidelines for security of cloud services
- NIST SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations (+ SP 800-161 Rev. 1 (Draft))
- PCI DSS Information Supplement: Third-Party Security Assurance
- The ISF Supply Chain Assurance Framework (SCAF)
- ISO 37500 Guidance on outsourcing

ISO 27036

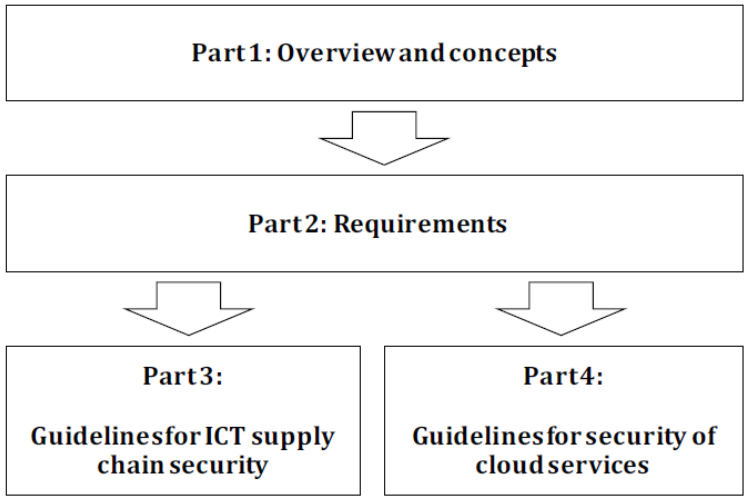


Figure 2 — ISO/IEC 27036 Architecture

ISO 27036-1 provides an overview of the guidance intended to assist organizations in securing their information and information systems within the context of supplier relationships.

ISO 27036-2:

a) specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships;

b) facilitates mutual understanding of the other party's approach to information security and tolerance for information security risks;

c) reflects the complexity of managing risks that can have information security impacts in supplier and acquirer relationships;

d) is intended to be used by any organization willing to evaluate the information security in supplier or acquirer relationships;

e) is not intended for certification purposes;

f) is intended to be used to set a number of defined information security objectives applicable to a supplier and acquirer relationship that is a basis for assurance purposes.

Examples of IS risks

Table 1 — Example information security risks for acquiring products

No.	Type	Description
1	Information security feature	In the case where supplied products have a vulnerability, the acquirer's derived products, services or processes will be vulnerable.
2	Quality	Poor quality of supplied products can cause information security weakness of the acquirer's derived products, services and processes.
3	Intellectual property rights	Unidentified intellectual property rights can cause later dispute in relation with the acquirer's derived products or services.
4	Authenticity	In the case where fake or fraudulent products were supplied, the acquirer's expectation for an information security feature and the quality and identification of intellectual property rights are threatened with a likelihood of an information security weakness introduced and a loss in the business relationship confidence.
5	Assurance	Without assurance of appropriate information security features, product quality, and identification of intellectual property rights and authenticity, the acquirer lacks confidence in reliance upon the supplier's products.

Table 2 — Example information security risks for acquiring services

No.	Type	Description	Example Use Case(s)
1	Physical access onsite	Supplier has physical access to the information processing facilities of the acquirer but does not have logical access	Security guard service, delivery services, a cleaning service or an equipment maintenance service
2	Access to information and information systems onsite	Supplier personnel are onsite and have logical access to information and information systems of the acquirer, through the use of acquirer's equipment	Outsourced expertise working onsite and integrated in acquirer's teams
3	Remote access to in-house information and information systems	Supplier has remote access to information and information systems of the acquirer	Remote development and maintenance activities, remote information system and equipment management, logistics, call centre operation, automated facilities management systems
4	Processing of information offsite	Information under the responsibility of the acquirer is processed by the supplier offsite, using applications and systems under the control and the management of the supplier	Consulting (market research, sales promotion, technical studies, etc.), information processing, R&D, manufacturing , storage and archival, application service (ASP), Business Process as a Service (BPaaS) such as travel or financial services, Infrastructure as a Service (IaaS) or Software as a Service (SaaS) providers
5	Applications offsite	Applications operated by the acquirer are running PaaS or IaaS	Platform as a Service (PaaS) providers if supplier provides development platform or IaaS providers if supplier provides network, compute and storage services
6	Equipment offsite	Equipment dedicated to the acquirer and owned by the acquirer are hosted offsite, on the supplier site	Offsite hosting of information systems housing or IaaS
7	Storage of information offsite	Acquirer outsources the storage of information to a supplier for offsite retention or archive	Use of storage service to maintain backup copies of information generated by in-house information processing
8	Source code escrow	Services involving supplier artefacts used by the acquirer are held in escrow by a trusted third party and are made available to the acquirer under defined circumstances	Source code held by an independent third party to maintain usefulness of software by the acquirer in the case that the supplier of the software goes out of business

By ISO 27036-1

Text of Clauses 6.1 to 6.4, and of Clauses 7.1 to 7.5 is structured in tables which need to be interpreted as follows:

Acquirer
Text specific to the acquirer.

Supplier
Text specific to the supplier.

Acquirer	**Supplier**
Text specific to both acquirer and supplier, unless explicitly stated.	
Text specific to the acquirer.	Text specific to the supplier.

By ISO 27036-2

These requirements are structured given following supplier relationship life cycle processes:

a) Supplier relationship planning process;

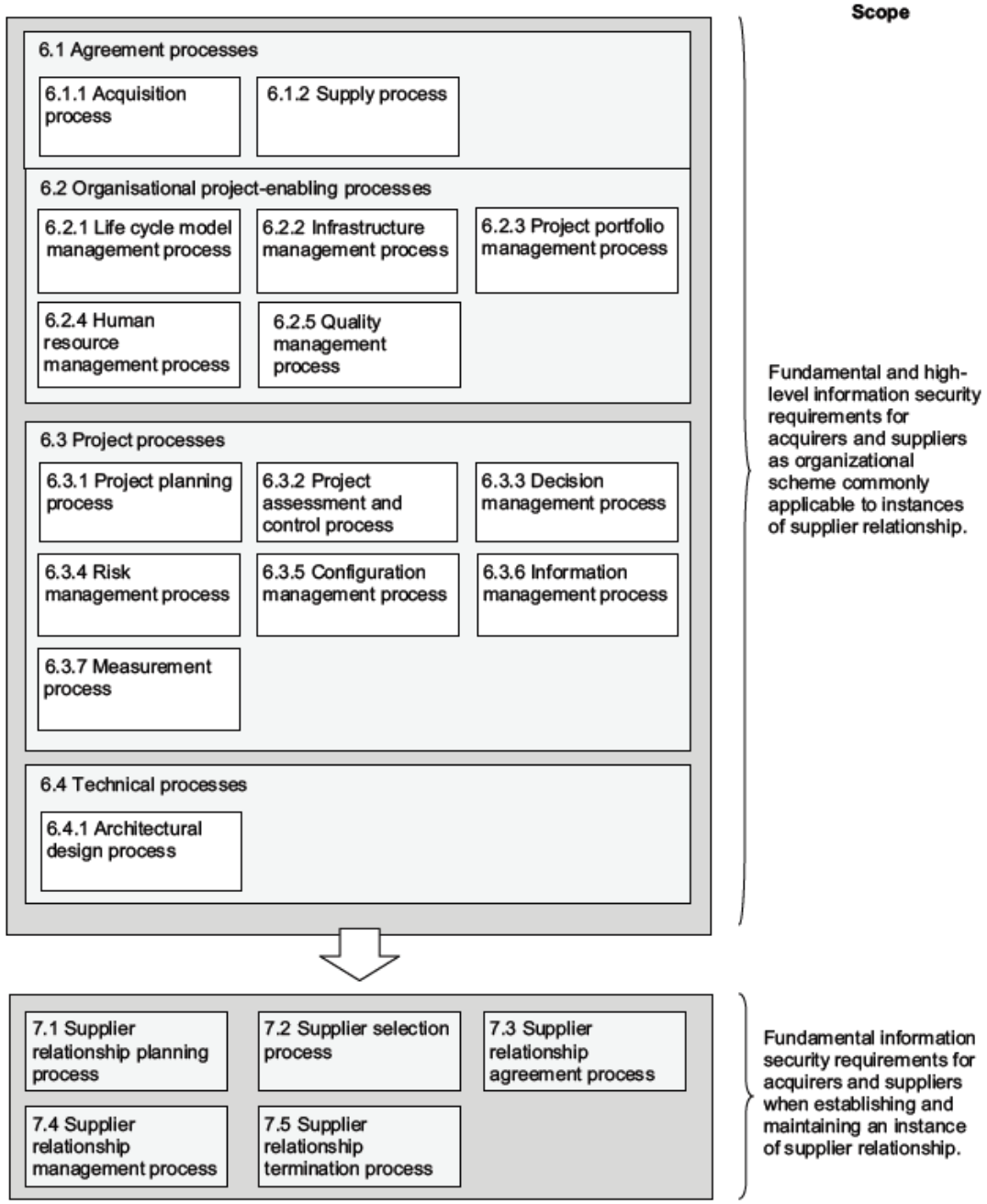
b) Supplier selection process;

c) Supplier relationship agreement process;

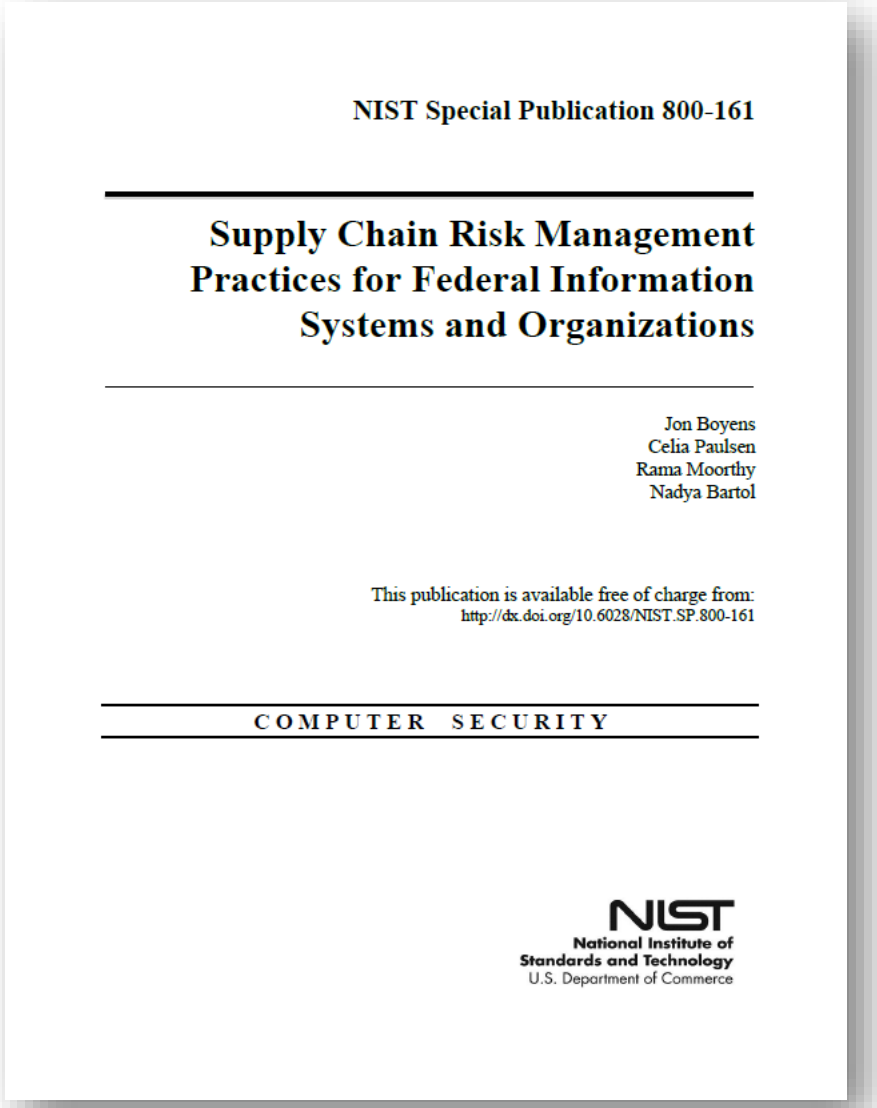
d) Supplier relationship management process;

e) Supplier relationship termination process.

By ISO 27036-2



NIST SP 800-161



NIST SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations

The purpose of this publication is to provide guidance to federal agencies on identifying, assessing, selecting, and implementing **risk management processes and mitigating controls** throughout their organizations to help manage **ICT supply chain risks**.

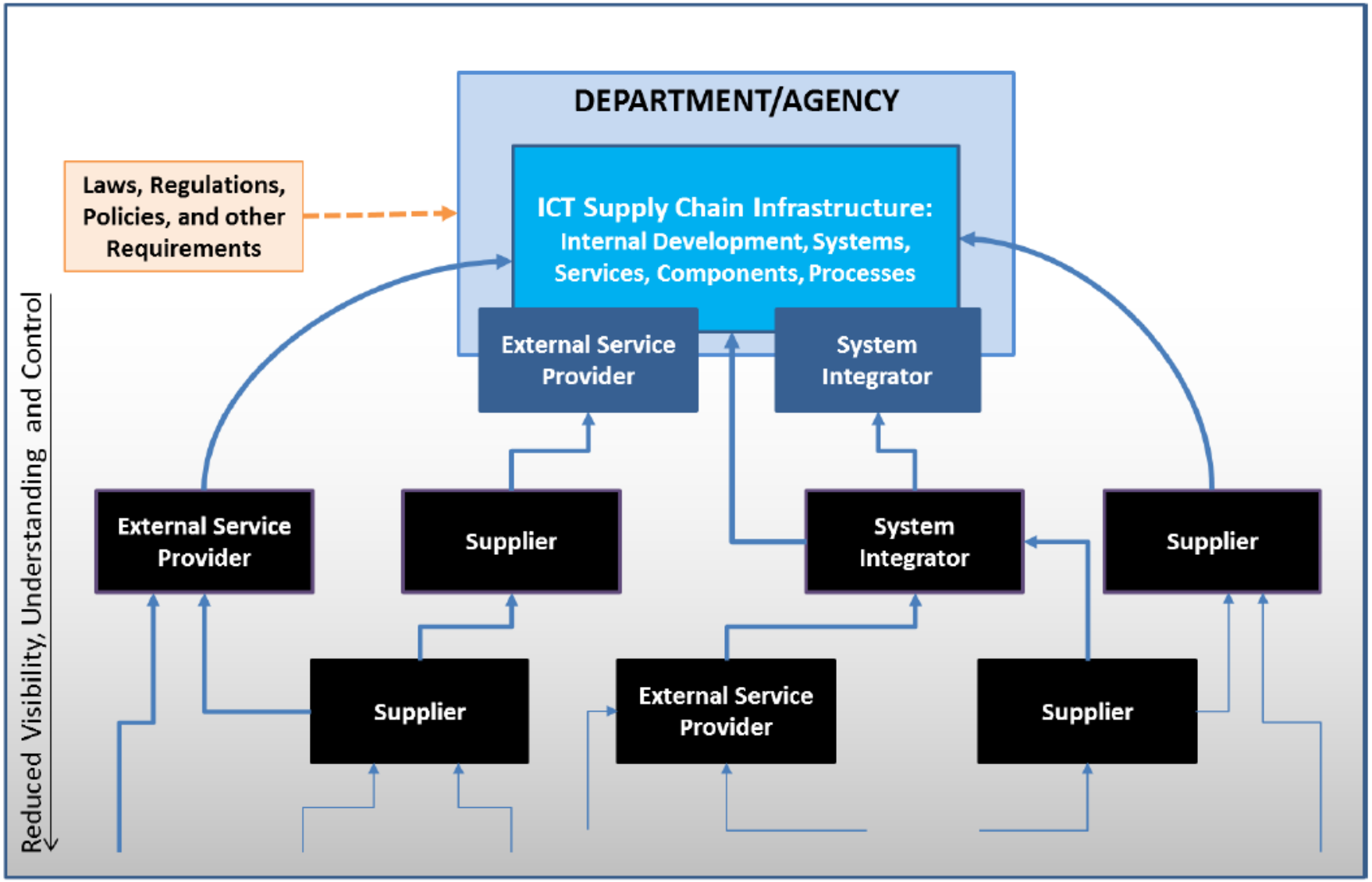


Figure 1-2: Federal Agency Relationships with System Integrators, Suppliers, and External Service Providers with Respect to the Scope of NIST SP 800-161.

NIST SP 800-161

Figure 1-1: Four Pillars of ICT SCRM

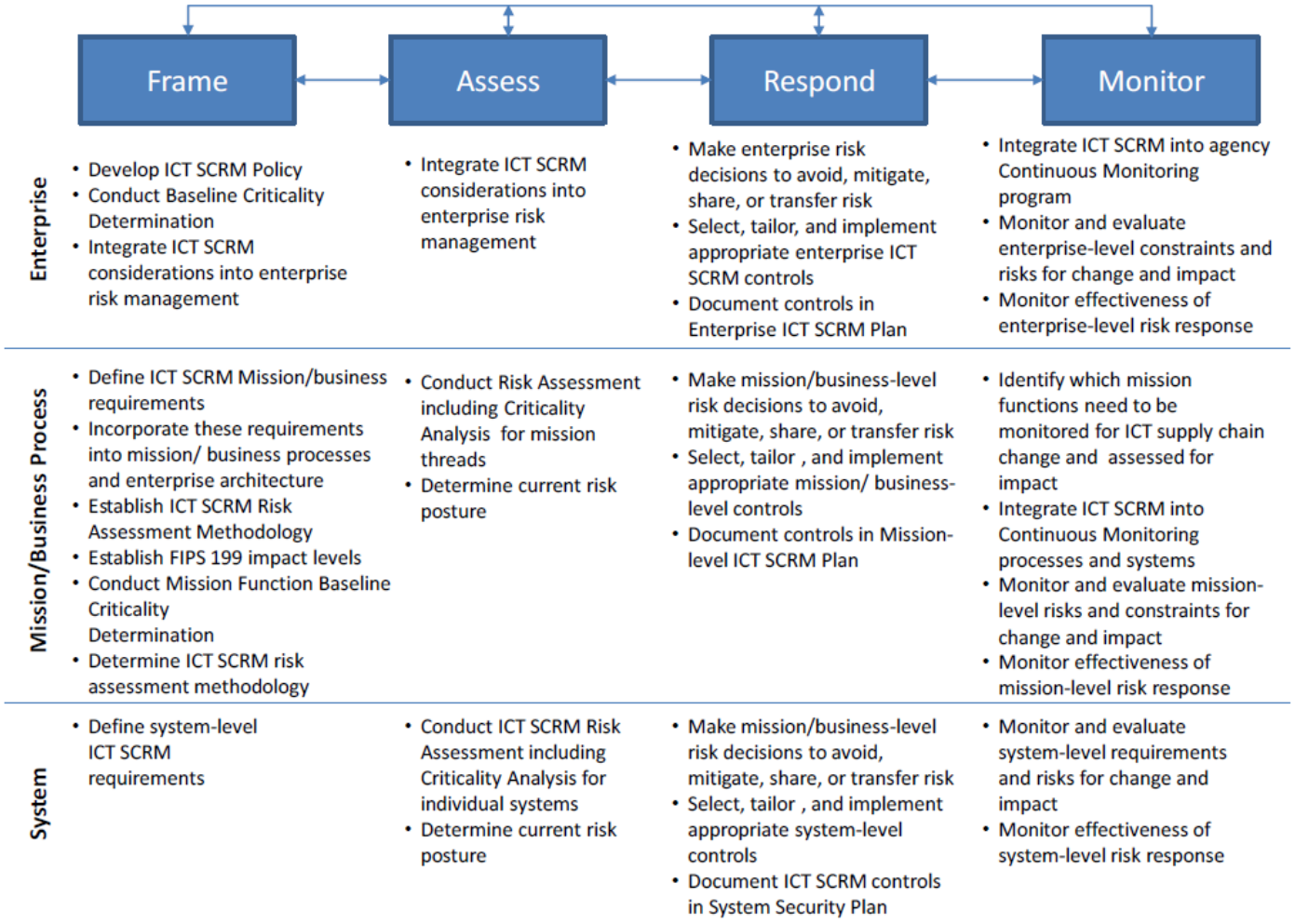


Figure 2-4: ICT SCRM Activities in Risk Management Process

The following are specific examples of the multidisciplinary foundational **practices that can be implemented** incrementally to improve an organization's ability to develop and implement more advanced ICT SCRM practices:

- Implement a risk management hierarchy and risk management process including an organization-wide risk assessment process
- Establish an organization governance structure that integrates ICT SCRM requirements and incorporates these requirements into the organizational policies
- Establish consistent, well-documented, repeatable processes for determining impact levels
- Use risk assessment processes after the impact level has been defined, including criticality analysis, threat analysis, and vulnerability analysis
- Implement a quality and reliability program that includes quality assurance and quality control process and practices
- Establish a set of roles and responsibilities for ICT SCRM that ensures that the broad set of appropriate stakeholders are involved in decision making, including who has the required authority to take action, who has accountability for an action or result, and who should be consulted and/or informed (e.g., Legal, Risk Executive, HR, Finance, Enterprise IT, Program Management/System Engineering, Information Security, Acquisition/procurement, supply chain logistics, etc.)
- Ensure that adequate resources are allocated to information security and ICT SCRM to ensure proper implementation of guidance and controls
- Implement consistent, well-documented, repeatable processes for system engineering, ICT security practices, and acquisition
- Implement an appropriate and tailored set of baseline information security controls in NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Establish internal checks and balances to assure compliance with security and quality requirements
- Establish a supplier management program including, for example, guidelines for purchasing directly from qualified original equipment manufacturers (OEMs) or their authorized distributors and resellers
- Implement a tested and repeatable contingency plan that integrates ICT supply chain risk considerations to ensure the integrity and reliability of the supply chain including during adverse events (e.g., natural disasters such as hurricanes or economic disruptions such as labor strikes); and
- Implement a robust incident management program to successfully identify, respond to, and mitigate security incidents. This program should be capable of identifying causes of security incidents, including those originating from the ICT supply chain

Other frameworks

- COBIT 2019 (APO10. Managed Vendors)
- Vendor Management: Using COBIT 5
- ISO/IEC 20000-1:2018 Information technology. Service management. Part 1: Service management system requirements (8.3.4 Supplier management)
- ITIL v4 Service Design (Supplier Management)
- Guide to the Project Management Body of Knowledge 6, PMBOK® Guide) (Project Procurement Management processes)

COBIT 2019. APO10 — Managed Vendors

Description: Manage I&T-related products and services provided by all types of vendors to meet enterprise requirements. This includes the search for and selection of vendors, management of relationships, management of contracts, and reviewing and monitoring of vendor performance and vendor ecosystem (including upstream supply chain) for effectiveness and compliance.

Purpose: Optimize available I&T capabilities to support the I&T strategy and road map, minimize the risk associated with nonperforming or noncompliant vendors, and ensure competitive pricing.

APO10.01 Identify and evaluate vendor relationships and contracts.

Continuously search for and identify vendors and categorize them into type, significance and criticality. Establish criteria to evaluate vendors and contracts. Review the overall portfolio of existing and alternative vendors and contracts.

APO10.02 Select vendors.

Select suppliers according to a fair and formal practice to ensure a viable best fit based on specified requirements. Requirements should be optimized with input from potential suppliers.

APO10.03 Manage vendor relationships and contracts.

Formalize and manage the supplier relationship for each supplier. Manage, maintain and monitor contracts and service delivery. Ensure that new or changed contracts conform to enterprise standards and legal and regulatory requirements. Deal with contractual disputes.

APO10.04 Manage vendor risk.

Identify and manage risk relating to vendors' ability to continually provide secure, efficient and effective service delivery. This also includes the subcontractors or upstream vendors that are relevant in the service delivery of the direct vendor.

APO10.05 Monitor vendor performance and compliance.

Periodically review overall vendor performance, compliance to contract requirements and value for money. Address identified issues.

COBIT 2019: Inputs and Outputs, RACI

C. Component: Information Flows and Items (see also Section 3.6)

Management Practice	Inputs		Outputs	
	From	Description	Description	To
APO10.01 Identify and evaluate vendor relationships and contracts.	Outside COBIT	Vendor contracts	Vendor catalog	BAI02.02
			Potential revisions to vendor contracts	Internal
			Vendor significance and evaluation criteria	Internal
APO10.02 Select vendors.	BAI02.02	High-level acquisition/ development plan	Vendor RFIs and RFPs	BAI02.01; BAI02.02
			RFI and RFP evaluations	BAI02.02
			Decision results of vendor evaluations	vendor evaluations BAI02.02; EDM04.01
APO10.03 Manage vendor relationships and contracts.	BAI03.04	Approved acquisition plan	Results and suggested improvements	Internal
			Communication and review process	Internal
			Vendor roles and responsibilities	Internal
APO10.04 Manage vendor risk.	APO12.04	• Risk analysis and risk profile reports for stakeholders • Results of third-party risk assessments	Identified vendor delivery risk	APO12.01; APO12.03; BAI01.01; BAI11.01
			Identified contract requirements to minimize risk	Internal
APO10.05 Monitor vendor performance and compliance.			Vendor compliance monitoring criteria	Internal
			Vendor compliance monitoring review results	MEA01.03

B. Component: Organizational Structures

Key Management Practice	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	I&T Governance Board	Enterprise Risk Committee	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Privacy Officer	Legal Counsel
APO10.01 Identify and evaluate vendor relationships and contracts.		R	R	R	A				R				R
APO10.02 Select vendors.		R	R	R	A		R	R	R	R	R	R	
APO10.03 Manage vendor relationships and contracts.		R	R	R	A		R	R	R	R			R
APO10.04 Manage vendor risk.	R	R	R	R	A	R	R	R	R	R	R	R	
APO10.05 Monitor vendor performance and compliance.	R	R	R	R	A	R	R	R	R	R			R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

Vendor Management: Using COBIT5

This publication on **vendor management** provides additional and more detailed practical guidance and facilitates the vendor management process for IT and business professionals.

The first action to mitigate vendor-related risk is to establish an effective **vendor management process** with goals and objectives that ensure the following:

- Vendor management strategy is consistent with enterprise goals.
- Effective cooperation and governance models are in place.
- Service, quality, cost and business goals are clear.
- All parties perform as agreed.
- Vendor risk is assessed and properly addressed.
- Vendor relationships are working effectively, as measured according to service objectives.

Figure 1—Life Cycle of the Contractual Relationship

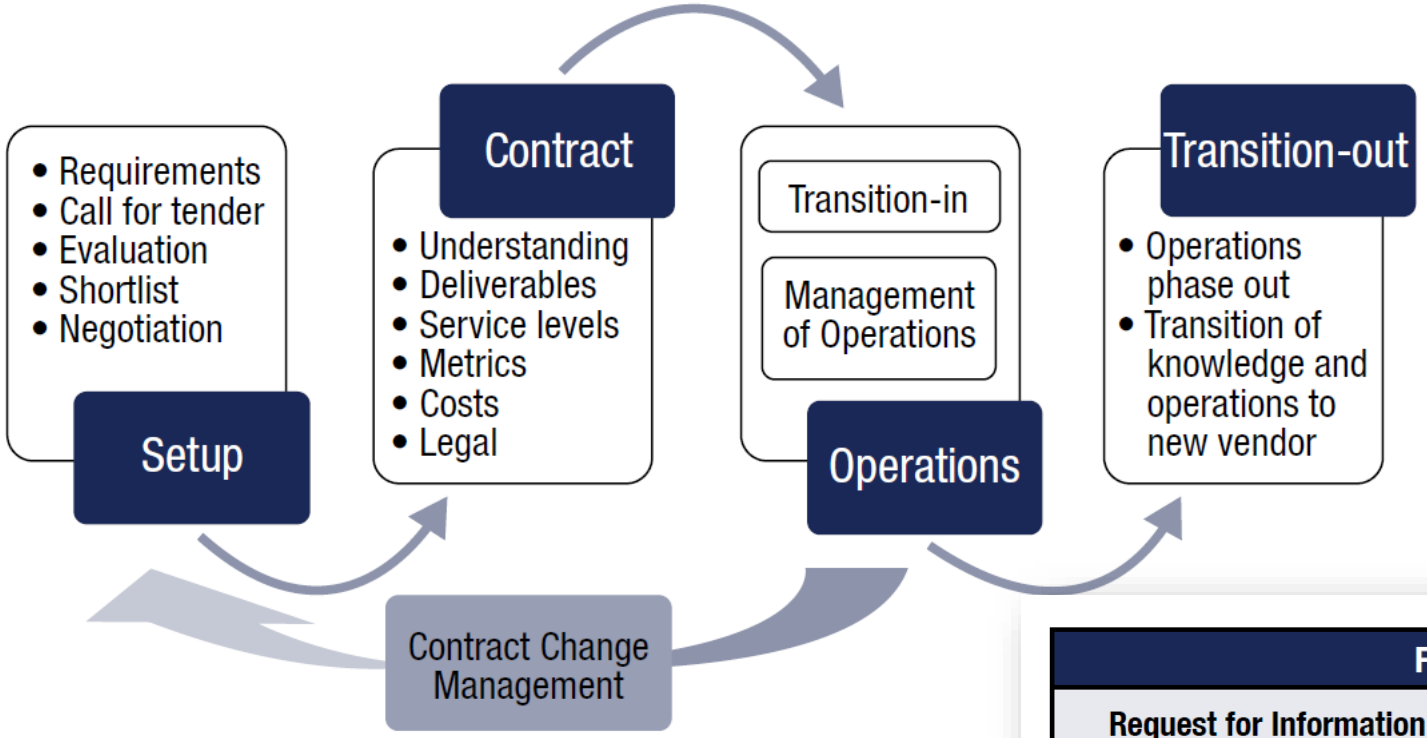


Figure 8—Information Items in the Vendor Relationship Life Cycle

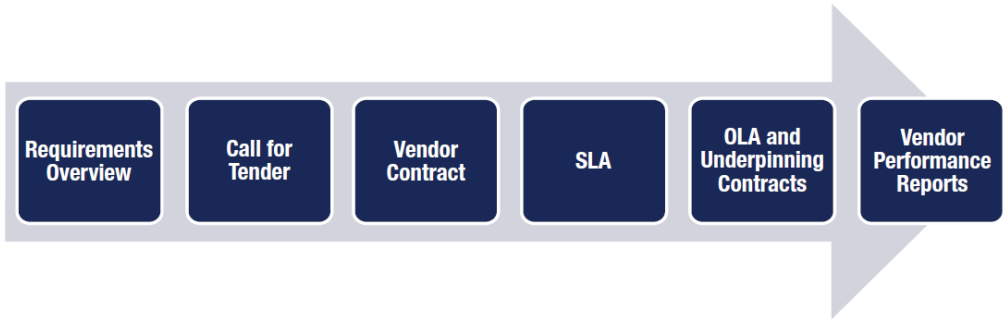


Figure 2—Bidding Document Comparison

Request for Information (RFI)	Request for Quotation (RFQ)	Request for Proposal (RFP)
• Educational tool • Used to gather information when product, services or requirements are not fully understood • Low complexity (easier to prepare, requires less effort than RFP) • Less formal than RFP • Can be used as input for RFP	• Price comparison tool • Used when customer understands products, services, requirements and market conditions • Medium complexity (easier to prepare, requires less effort than RFP, requires clear understanding of requirements) • Semiformal • Simplifies vendor comparison by focusing on price	• Formal evaluation tool • Used when customer understands products or services and has well-defined requirements • High complexity (requires significant time invested in documenting requirements and evaluation criteria) • Can be used before sending RFQ

Figure 3—Vendor Management RACI Chart				
Stakeholder	Contractual Relationship Life Cycle			
	Setup	Contract	Operations	Transition-out
C-level executives	A	A	A	A
Business process owners	R	R	I	R
Procurement	R	R	I	R
Legal	R	R	C	C
Risk function	C	C	R	R
Compliance and audit	C	C	C	C
IT	R	R	R	R
Security	R	C	R	C
Human resources (HR)	C	C	C	C

22 mitigation actions by COBIT

1. Diversify sourcing strategy to avoid overreliance or vendor lockin
2. Establish policies and procedures for vendor management
3. Establish a vendor management governance model
4. Set up a vendor management organization within the enterprise
5. Foresee requirements regarding the skills and competencies of the vendor employees
6. Use standard documents and templates
7. Formulate clear requirements
8. Perform adequate vendor selection
9. Cover all relevant life-cycle events during contract drafting
10. Determine the adequate security and controls needed during the relationship
11. Set up SLAs
12. Set up operating level agreements (OLAs) and underpinning contracts
13. Set up appropriate vendor performance/service level monitoring and reporting
14. Establish a penalties and reward model with the vendor
15. Conduct adequate vendor relationship management during the life cycle
16. Review contracts and SLAs on a periodic basis
17. Conduct vendor risk management
18. Perform an evaluation of compliance with enterprise policies
19. Perform an evaluation of vendor internal controls
20. Plan and manage the end of the relationship
21. Use a vendor management system
22. Create data and hardware disposal stipulations

ISO/IEC 20000 Service management

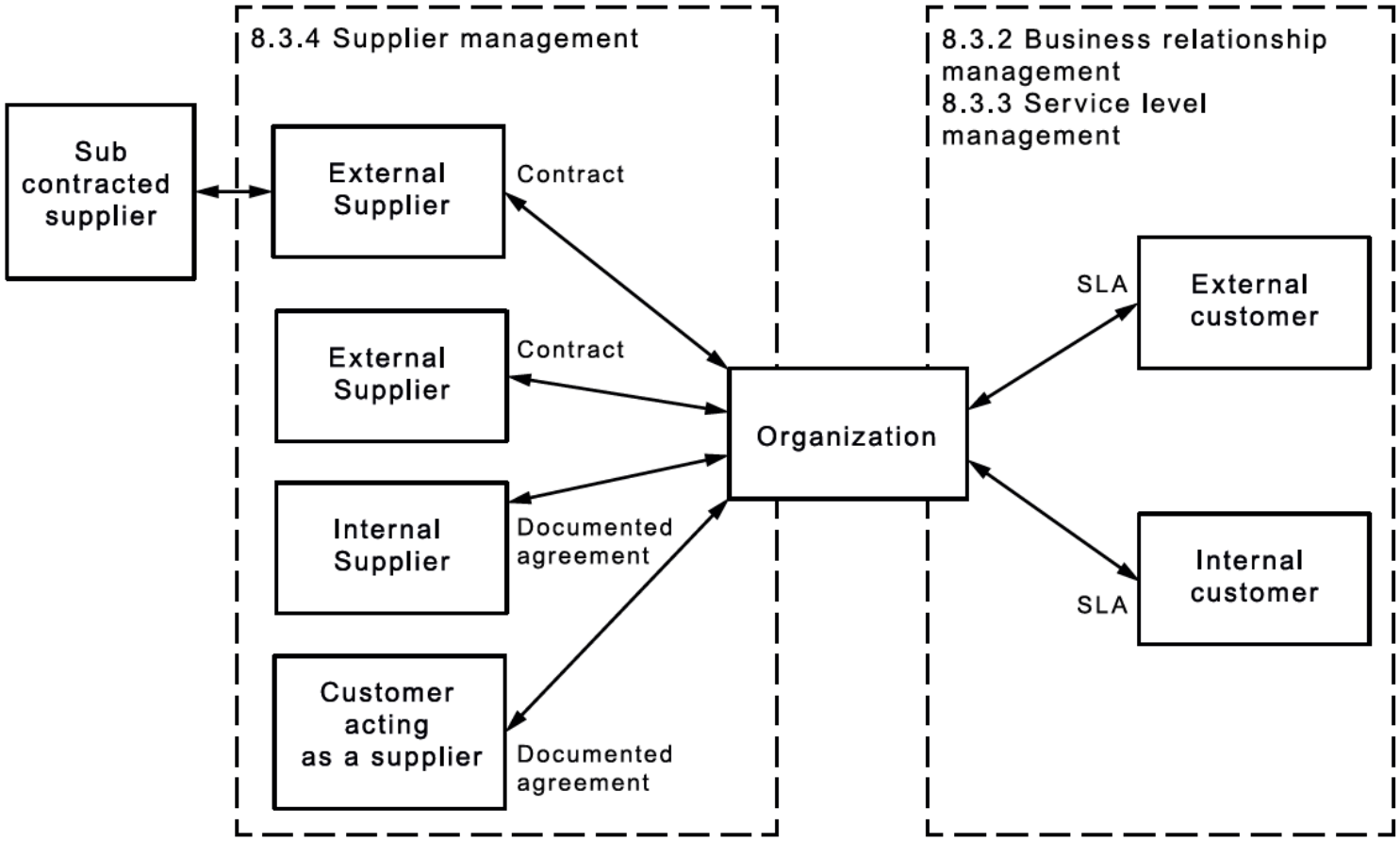


Figure 2 Relationships and agreements between parties involved in the service lifecycle

8.3.4 Supplier management

8.3.4.1 Management of external suppliers

The organization shall have one or more designated individuals responsible for managing the relationship, contracts and performance of external suppliers.

For each external supplier, the organization shall agree a documented contract. The contract shall include or contain a reference to:

a) scope of the services, service components, processes or parts of processes to be provided or operated by the external supplier;

b) requirements to be met by the external supplier;

c) service level targets or other contractual obligations;

d) authorities and responsibilities of the organization and the external supplier.

The organization shall assess the alignment of service level targets or other contractual obligations for the external supplier against SLAs with customers, and manage identified risks.

The organization shall define and manage the interfaces with the external supplier.

At planned intervals, the organization shall monitor the performance of the external supplier. Where service level targets or other contractual obligations are not met, the organization shall ensure that opportunities for improvement are identified.

At planned intervals, the organization shall review the contract against current service requirements. Changes identified for the contract shall be assessed for the impact of the change on the SMS and the services before the change is approved.

Disputes between the organization and the external supplier shall be recorded and managed to closure.

8.3.4.2 Management of internal suppliers and customers acting as a supplier

For each internal supplier or customer acting as a supplier, the organization shall develop, agree and maintain a documented agreement to define the service level targets, other commitments, activities and interfaces between the parties.

At planned intervals, the organization shall monitor the performance of the internal supplier or the customer acting as a supplier. Where service level targets or other agreed commitments are not met, the organization shall ensure that opportunities for improvement are identified.

Summary. Key topics

1. Governance model (roles and responsibilities)
2. Information security policy for supplier relationships / Supplier management framework
3. Information risk assessments of suppliers
4. Information security requirements
5. Supplier selection criteria
6. Procurement processes
7. Register of suppliers
8. Supplier Contracts and Agreements (+SLA/OLA)
9. Confidentiality agreement (NDA)
10. Information classification, labeling and handling
11. Information transfer
12. Communication and notification
13. Incident handling
14. Change management (and notification)
15. Monitoring, evaluation and assurance activities (e.g. audits)
16. Cloud security management
17. Core cloud security controls
18. Outsourcing and Outstaffing
19. Personal Data protection and compliance
20. Cross-border/multi-jurisdictional legislative and regulatory requirements
21. Exit strategy / termination process (return, transfer, or verified secure destruction of physical assets and revocation of access rights)

Thanks!