Chapter 15 – Supplier relationships

15.1.1 Information security policy for supplier relationships - Security requirements should be agreed with the supplier and documented. The control which addresses processes and procedures should be identified and documented in a policy, includes identifying and documenting the types of suppliers; a standardized process and lifecycle; minimum security requirements, processes and procedures for monitoring adherence to established requirements; accuracy and completeness to ensure information integrity; types of obligations applicable to suppliers; handling incidents and contingencies; resilience and recovery and contingency arrangements for availability of information; awareness training for the organization's personnel on policies, processes and procedures; and for organization's personnel interacting with supplier personnel on rules of engagement and behavior; conditions under which security requirements and controls will be documented in an agreement; managing transitions of information, information processing facilities.

15.1.2. Addressing security within supplier agreements - Description of information to be provided; classification of information; legal and regulatory requirements; obligation of each contractual party; rules of acceptable use of information; explicit list of supplier's authorized personnel; information security policies; incident management requirements and procedures; training and awareness requirements; relevant regulations for sub-contracting and for partners; screening requirements; right to audit the supplier process and controls; defect and conflict resolution processes; supplier's obligation to periodically deliver report, and to comply with the organization's security requirements.

15.1.3. Information and communication technology supply chain – agreements should include: defining security requirements; the suppliers propagate the requirements and appropriate security practices throughout the supply chain; implementing a monitoring acceptable methods; implementing a process for identifying product or service components; obtaining assurance that critical components and their origin can be traced; and on the delivered technology products functionality; defining rules for information sharing; implementing specific processes for the technology component lifecycle and availability and associated security risks.

15.2. Supplier service delivery management – to maintain an agreed level of information security

15.2.1. Monitoring and review of supplier services - Organizations should regularly monitor, review and audit supplier service delivery to manage security incidents and problems. This should involve monitoring service performance levels; review reports and conduct audits of suppliers; provide information about security incidents; review supplier audit trails and records; resolve and manage identified problems; review security aspects of supplier's relationships; maintains sufficient service capability of supplier.

15.2.2. Managing changes to supplier services - changes to supplier agreements; changes made by the organization to implement; changes in supplier services to implement are taken into consideration.

Chapter 16: Information security incident management

16.1. Management of information security incidents and improvements - Ensure consistent and effective approach to the management of information security incidents.

16.1.1. Responsibilities and procedures - Procedures are developed and communicated adequately to ensure competent personnel, a point of contact for incident's detection and reporting; appropriate contacts with authorities to handle security incidents issues; reporting procedures should include preparing security event reporting forms; reference to formal disciplinary process; suitable feedback processes.

16.1.2. Reporting information security events - All employees and contractors should be made aware of their responsibility to report security events; the procedure for reporting and the point of contact. Situations to be considered for reporting include: ineffective security control that are breach of information integrity, confidentiality or availability expectations; human errors, non-compliance with policies or guidelines; breaches of physical security arrangements; uncontrolled system changes; malfunctions of software or hardware and access violations.

16.1.3. Reporting information security weaknesses - Any observed or suspected security weaknesses in systems or services are required to be noted and be reported by employees and contractors.

16.1.4. Assessment of and decision on information security events - Security events should be assessed and be decided by the point of contact; and be recorded for future reference and verification.

16.1.5. Response to information security incidents - Security incidents should be responded per the procedures. It includes: collecting evidence; conducting security forensics analysis; escalation; response activities are properly logged for late analysis; the existence of security incident should be communicated to internal/external people; dealing with weaknesses found to cause/contribute to the incident; the incident successfully dealt with be formally closed and recorded. Source of the incident should be identified.

16.1.6. Learning from information security incidents - Knowledge gained from analyzing and resolving security incidents should be used to reduce the likelihood or impact of future incidents.

16.1.7. Collection of evidence - Procedures for identification, collection, acquisition and preservation of information, which can serve as evidence, should be defined. Procedures for disciplinary and legal action should be developed. The procedure should take account of chain of custody; safety of evidence and personnel; roles and responsibilities of personnel; competency of personnel; documentation; and briefing.

Chapter 17: information security aspects of business continuity management

17.1 information security continuity – should be embedded in the system

17.1.1. Planning information security continuity - Information security and continuity of management in adverse situations should be determined.

17.1.2. Implementing information security continuity - The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

17.1.3. Verify, review and evaluate information security continuity - The established and implemented information security continuity controls should be verified at regular intervals to ensure that they are valid and effective during adverse situations.

17.2. Redundancies – ensure availability of information processing facilities

17.2.1. Availability of information processing facilities – should be implemented with redundancy to meet availability requirements. Identify business requirements for availability of information systems, where availability cannot be guaranteed using the existing system architecture, redundant components or architectures should be considered.

Chapter 18: Compliance

18.1. Compliance with legal and contractual requirements – to avoid breaches of legal, statutory, regulatory or contractual obligations

18.1.1. Identification of applicable legislation and contractual requirements – relevant statutory, regulatory, contractual requirements and the organization's approach to meet requirements should be explicitly identified, documented and kept up to date for each information system and the organization.

18.1.2. Intellectual property rights – procedures should be implemented related to rights and use of proprietary software products includes publishing property rights; compliance policy; acquiring software only through known reputable sources; maintaining awareness of policies to protect intellectual property rights; appropriate asset registers and identifying all assets; proof and evidence of ownership of licenses, master disks, manuals, etc; implementing controls; carrying out reviews only authorized software and licenses products are installed; providing policy for appropriate license conditions; providing a policy for disposing/ transferring software to others; complying with terms and conditions for software and information from public networks; not duplicating, converting to another format/extracting from commercial recordings; not copying in full or in part.

18.1.3. Protection of records – records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, per legislator, regulatory, contractual and business requirements.

18.1.4. Privacy and protection of personally identifiable information - the policy should be communicated to all persons. It requires appropriate management structure and control to handle it; awareness of the privacy principles should be dealt with per relevant legislation and regulations. Technical and organizational measures should be implemented.

18.1.5. Regulation of cryptographic controls – the control should be used in compliance with relevant agreements, legislation and regulations; include restrictions on import or export of computer hardware and software for performing cryptographic functions and designed to have cryptographic functions added to it; restrictions on the usage of encryption; mandatory or discretionary methods of access by the countries' authorities to information encrypted by hardware or software to provide confidentiality of content.

18.2. Independent security reviews -implemented and operated per the organizational policies and procedures.

18.2.1. Independent review of information security – the organization's approach to managing information security and its implementation should be reviewed independently at planned intervals or when changes occur.

18.2.2. Compliance with security policies and standards – regularly review the compliance of processing and procedures with appropriate security policies, standards. Causes should be identified; evaluate; implement appropriate corrective actions; and review the corrective actions taken to verify its effectiveness; identify deficiencies/weaknesses, when any none-compliance found.

18.2.3. Technical compliance review – information systems should be regularly reviewed for compliance security policies and standards. It is carried out by competent, authorized persons. Examined operational systems to ensure that hardware and software controls have been correctly implemented.

Questions

1. Do you include terms and conditions in the agreement with the suppliers to mitigate the risks associated with supplier's access to the organization's assets?
2. Do you have processes and procedures in the agreement to be implemented by the supplier?
3. Do you have any practice to monitoring and review of supplier services?
4. Do you have information security incident management program?
5. Do you have management responsibilities and procedures with regard to information security incident management are?
6. Did you develop and follow procedures to deal with evidence for the purposes of disciplinary and legal action?
7. Do you have the continuity of information security management program?
8. Do you apply guidelines for implementation of continuity for information security?
9. Do you ensure compliance with legislative, regulatory and contractual requirements?
10. What have you done to protect any material that may be considered intellectual property?