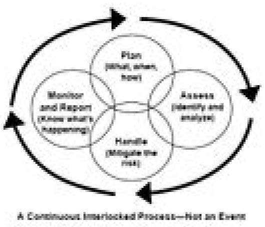
IT risk management

IT risk management is the application of risk management methods to information technology in order to manage IT risk, i.e.:



Risk management elements

> *The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise or organization*

IT risk management can be considered a component of a wider enterprise risk management system.[1]

The establishment, maintenance and continuous update of an information security management system (ISMS) provide a strong indication that a company is using a systematic approach for the identification, assessment and management of information security risks.[2]

Different methodologies have been proposed to manage IT risks, each of them divided into processes and steps.[3]

According to the Risk IT framework,[1] this encompasses not only the negative impact of operations and service delivery which can bring destruction or reduction of the value of the organization, but also the benefit enabling risk associated to missing opportunities to use technology to enable or enhance business or the IT project management for aspects like overspending or late delivery with adverse business impact.

Because risk is strictly tied to uncertainty, decision theory should be applied to manage risk as a science, i.e. rationally making choices under uncertainty.

Generally speaking, risk is the product of likelihood times impact (Risk = Likelihood * Impact).[4]

The measure of an IT risk can determined as a product of threat, vulnerability and asset values:[5]

$$\mathbf{Risk} = \mathbf{Threat} \times \mathbf{Vulnerability} \times \mathbf{Asset}$$

A more current risk management framework for IT Risk would be the TIK framework:

$$\mathbf{Risk} = ((\mathbf{Vulnerability} \times \mathbf{Threat})/\mathbf{Counter\ measure}) \times \mathbf{Asset\ value\ at\ risk}$$

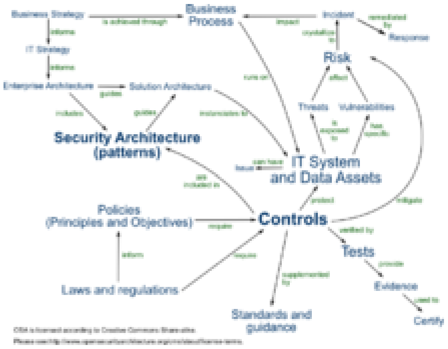
The *process* of risk management is an ongoing iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerabilities emerge every day. The choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

Definitions

The Certified Information Systems Auditor Review Manual 2006 produced by ISACA, an international professional association focused on IT Governance, provides the following definition of risk management: *"Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization."*[6]

Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems *and data that support their organizations' missions. This process is not unique to the IT environment; indeed it pervades decision-making in all areas of our daily lives.*[7]

The head of an organizational unit must ensure that the organization has the capabilities needed to accomplish its mission. These mission owners must determine the security capabilities that their IT systems must have to provide the desired level of mission support in the face of real world threats. Most organizations have tight budgets for IT security; therefore, IT security spending must be reviewed as thoroughly as other management decisions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.[7]



Relationships between IT security entity

Risk management in the IT world is quite a complex, multi faced activity, with a lot of relations with other complex activities. The picture to the right shows the relationships between different related terms.

The American National Information Assurance Training and Education Center defines risk management in the IT field as:[8]

1. *The total process to identify, control, and minimize the impact of uncertain events. The objective of the risk management program is to reduce risk and obtain and maintain DAA approval. The process facilitates the management of security risks by each level of management throughout the system life cycle. The approval process consists of three elements: risk analysis, certification, and approval.*

2. *An element of managerial science concerned with the identification, measurement, control, and minimization of uncertain events. An effective risk management program encompasses the following four phases:*
    1. a *Risk assessment, as derived from an evaluation of threats and vulnerabilities.*
    2. *Management decision.*
    3. *Control implementation.*
    4. *Effectiveness review.*
3. *The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems review.*
4. *The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.*

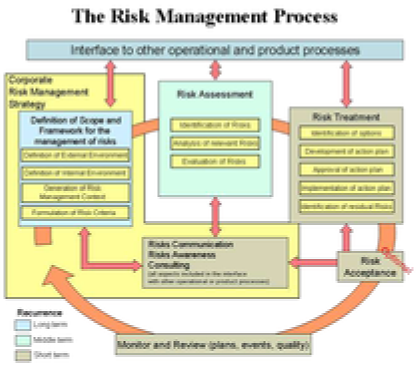
Risk management as part of enterprise risk management

Some organizations have and many others should have a comprehensive Enterprise risk management (ERM) in place. The four objective categories addressed, according to Committee of Sponsoring Organizations of the Treadway Commission (COSO) are:

- Strategy - high-level goals, aligned with and supporting the organization's mission
- Operations - effective and efficient use of resources
- Financial Reporting - reliability of operational and financial reporting
- Compliance - compliance with applicable laws and regulations

According to the Risk IT framework by ISACA,[9] IT risk is transversal to all four categories. The IT risk should be managed in the framework of Enterprise risk management: Risk appetite and Risk sensitivity of the whole enterprise should guide the IT risk management process. ERM should provide the context and business objectives to IT risk management

Risk management methodology


The Risk Management Process
Interface to other operational and product processes
Corporate Risk Management Strategy
Definition of Scope and Framework for the management of risks
Definition of External Environment
Definition of Internal Environment
Generation of Risk Management Context
Formulation of Risk Criteria
Risk Assessment
Identification of Risks
Analysis of relevant Risks
Evaluation of Risks
Risk Treatment
Identification of options
Development of action plan
Approval of action plan
Implementation of action plan
Identification of residual Risks
Risks Communication
Risks Awareness
Consulting
(all aspects included in the interface with other operational or product processes)
Risk Acceptance
Monitor and Review (plans, events, quality)
Recurrence
Long term
Middle term
Short term

ENISA: The Risk Management Process, according to ISO Standard 13335

Whilst a methodology does not describe specific methods ; nevertheless it does specify several processes (constitute a generic framework) that need to be followed. These processes may be broken down in sub-processes, they may be combined, or their sequence may change. A risk management exercise must carry out these processes in one form or another, The following table compares the processes foreseen by three leading standards.[3] The ISACA Risk IT framework is more recent. The Risk IT Practitioner-Guide[10] compares Risk IT and ISO 27005.

The term methodology means an organized set of principles and rules that drive action in a particular field of knowledge.[3]

The overall comparison is illustrated in the following table.

Risk management constituent processes

ISO/IEC 27005:2008	BS 7799-3:2006	NIST SP 800-39	Risk IT
Context establishment	Organizational context	Frame	RG and RE Domains more precisely • RG1.2 Propose IT risk tolerance, • RG2.1 Establish and maintain accountability for IT risk management • RG2.3 Adapt IT risk practices to enterprise risk practices, • RG2.4 Provide adequate resources for IT risk management, • RE2.1 Define IT risk analysis scope.
Risk assessment	Risk assessment	Assess	RE2 process includes: • RE2.1 Define IT risk analysis scope. • RE2.2 Estimate IT risk. • RE2.3 Identify risk response options. • RE2.4 Perform a peer review of IT risk analysis. In general, the elements as described in the ISO 27005 process are all included in Risk IT; however, some are structured and named differently.
Risk treatment	Risk treatment and management decision making	Respond	• RE 2.3 Identify risk response options • RR2.3 Respond to discovered risk exposure and opportunity
Risk acceptance			RG3.4 Accept IT risk
Risk communication	Ongoing risk management activities		• RG1.5 Promote IT risk-aware culture • RG1.6 Encourage effective communication of IT risk

			• RE3.6 Develop IT risk indicators.
Risk monitoring and review		Monitor	• RG2 Integrate with ERM. • RE2.4 Perform a peer review of IT risk analysis. • RG2.5 Provide independent assurance over IT risk management

Due to the probabilistic nature and the need of cost benefit analysis, IT risks are managed following a process that according to NIST SP 800-30 can be divided in the following steps:[7]

1. risk assessment,
2. risk mitigation, and
3. evaluation and assessment.

Effective risk management must be totally integrated into the Systems Development Life Cycle.[7]

Information risk analysis conducted on applications, computer installations, networks and systems under development should be undertaken using structured methodologies.[11]

Context establishment

This step is the first step in ISO ISO/IEC 27005 framework. Most of the elementary activities are foreseen as the first sub process of Risk assessment according to NIST SP 800–30. This step implies the acquisition of all relevant information about the organization and the determination of the basic criteria, purpose, scope and boundaries of risk management activities and the organization in charge of risk management activities. The purpose is usually the compliance with legal requirements and provide evidence of due diligence supporting an ISMS that can be certified. The scope can be an incident reporting plan, a business continuity plan.

Another area of application can be the certification of a product.

Criteria include the risk evaluation, risk acceptance and impact evaluation criteria. These are conditioned by:[12]

- legal and regulatory requirements
- the strategic value for the business of information processes

- stakeholder expectations
- negative consequences for the reputation of the organization

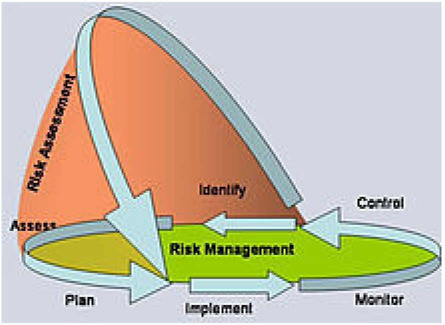
Establishing the scope and boundaries, the organization should be studied: its mission, its values, its structure; its strategy, its locations and cultural environment. The constraints (budgetary, cultural, political, technical) of the organization are to be collected and documented as guide for next steps.

Organization for security management

The set up of the organization in charge of risk management is foreseen as partially fulfilling the requirement to provide the resources needed to establish, implement, operate, monitor, review, maintain and improve an ISMS.[13] The main roles inside this organization are:[7]

- Senior Management
- Chief information officer (CIO)
- System and Information owners, such as the Chief Data Officer (CDO) or Chief Privacy Officer (CPO)
- the business and functional managers
- the Information System Security Officer (ISSO) or Chief information security officer (CISO)
- IT Security Practitioners
- Security Awareness Trainers

Risk assessment



ENISA: Risk assessment inside risk management

Risk Management is a recurrent activity that deals with the analysis, planning, implementation, control, and monitoring of implemented measurements and the enforced security policy. On the contrary, Risk Assessment is executed at discrete time points (e.g. once a year, on demand, etc.) and – until the performance of the next assessment – provides a temporary view of assessed risks and while parameterizing the entire Risk Management process. This view of the relationship of Risk Management to Risk Assessment is depicted in figure as adopted from OCTAVE.[2]

Risk assessment is often conducted in more than one iteration, the first being a high-level assessment to identify high risks, while the other iterations detailed the analysis of the major risks and other risks.

According to National Information Assurance Training and Education Center risk assessment in the IT field is:[8]

1. *A study of the vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. Managers use the results of a risk assessment to develop security requirements and specifications.*
2. *The process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations.*
3. *An identification of a specific ADP facility's assets, the threats to these assets, and the ADP facility's vulnerability to those threats.*
4. *An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events. The purpose of a risk assessment is to determine if countermeasures are adequate to reduce the probability of loss or the impact of loss to an acceptable level.*
5. *A management tool which provides a systematic approach for determining the relative value and sensitivity of computer installation assets, assessing vulnerabilities, assessing loss expectancy or perceived risk exposure levels, assessing existing protection features and additional protection alternatives or acceptance of risks and documenting management decisions. Decisions for implementing additional protection features are normally based on the existence of a reasonable ratio between cost/benefit of the safeguard and*

> *sensitivity/value of the assets to be protected. Risk assessments may vary from an informal review of a small scale microcomputer installation to a more formal and fully documented analysis (i. e., risk analysis) of a large scale computer installation. Risk assessment methodologies may vary from qualitative or quantitative approaches to any combination of these two approaches.*

ISO 27005 framework

Risk assessment receives as input the output of the previous step Context establishment; the output is the list of assessed risks prioritized according to risk evaluation criteria. The process can be divided into the following steps:[12]

- Risk analysis, further divided in:
  - Risk identification
  - Risk estimation
  - Risk evaluation

The following table compares these ISO 27005 processes with Risk IT framework processes:[10]

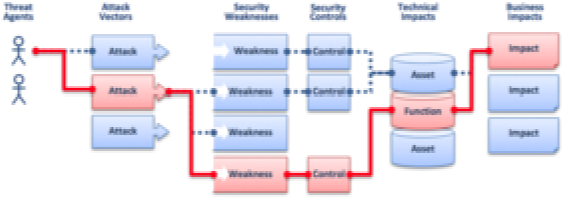
Risk assessment constituent processes

ISO 27005	Risk IT
Risk analysis	• RE2 Analyse risk comprises more than what is described by the ISO 27005 process step. RE2 has as its objective developing useful information to support risk decisions that take into account the business relevance of risk factors. • RE1 Collect data serves as input to the analysis of risk (e.g., identifying risk factors, collecting data on the external environment).
Risk identification	This process is included in RE2.2 Estimate IT risk. The identification of risk comprises the following elements: • Risk scenarios • Risk factors
Risk estimation	RE2.2 Estimate IT risk
Risk evaluation	RE2.2 Estimate IT risk

The ISO/IEC 27002:2005 Code of practice for information security management recommends the following be examined during a risk assessment:

- security policy,
- organization of information security,
- asset management,
- human resources security,
- physical and environmental security,
- communications and operations management,
- access control,
- information systems acquisition, development and maintenance, (see Systems Development Life Cycle)
- information security incident management,
- business continuity management, and
- regulatory compliance.

Risk identification



OWASP: relationship between threat agent and business impact

Risk identification states what could cause a potential loss; the following are to be identified:[12]

- assets, primary (i.e. Business processes and related information) and supporting (i.e. hardware, software, personnel, site, organization structure)
- threats

- existing and planned security measures
- vulnerabilities
- consequence
- related business processes

The output of sub process is made up of:

- list of asset and related business processes to be risk managed with associated list of threats, existing and planned security measures
- list of vulnerabilities unrelated to any identified threats
- list of incident scenarios with their consequences.

Risk estimation

There are two methods of risk assessment in information security field, quantitative and qualitative.[14]

Purely quantitative risk assessment is a mathematical calculation based on security metrics on the asset (system or application). For each risk scenario, taking into consideration the different risk factors a Single loss expectancy (SLE) is determined. Then, considering the probability of occurrence on a given period basis, for example the annual rate of occurrence (ARO), the Annualized Loss Expectancy is determined as the product of ARO and SLE.[5] It is important to point out that the values of assets to be considered are those of all involved assets, not only the value of the directly affected resource.
For example, if you consider the risk scenario of a Laptop theft threat, you should consider the value of the data (a related asset) contained in the computer and the reputation and liability of the company (other assets) deriving from the loss of availability and confidentiality of the data that could be involved. It is easy to understand that intangible assets (data, reputation, liability) can be worth much more than physical resources at risk (the laptop hardware in the example).[15] Intangible asset value can be huge, but is not easy to evaluate: this can be a consideration against a pure quantitative approach.[16]

Qualitative risk assessment (three to five steps evaluation, from Very High to Low) is performed when the organization requires a risk assessment be performed in a relatively short time or to meet a small budget, a significant quantity of relevant data is not available, or the persons performing the assessment don't have the sophisticated mathematical, financial, and risk assessment expertise required.[14] Qualitative risk assessment can be performed in a shorter period of time and with less data. Qualitative risk assessments are typically performed through interviews of a sample of personnel from all relevant groups within an organization charged with the security of the asset being assessed. Qualitative risk assessments are descriptive versus measurable. Usually a qualitative classification is done followed by a quantitative evaluation of the highest risks to be compared to the costs of security measures.

Risk estimation has as input the output of risk analysis and can be split in the following steps:

- assessment of the consequences through the valuation of assets
- assessment of the likelihood of the incident (through threat and vulnerability valuation)
- assign values to the likelihood and consequence of the risks

The output is the list of risks with value levels assigned. It can be documented in a risk register.

Risks arising from security threats and adversary attacks may be particularly difficult to estimate. This difficulty is made worse because, at least for any IT system connected to the Internet, any adversary with intent and capability may attack because physical closeness or access is not necessary. Some initial models have been proposed for this problem.[17]

During risk estimation there are generally three values of a given asset, one for the loss of one of the CIA properties: Confidentiality, Integrity, Availability.[18]

Risk evaluation

The risk evaluation process receives as input the output of risk analysis process. It compares each risk level against the risk acceptance criteria and prioritise the risk list with risk treatment indications.

NIST SP 800 30 framework

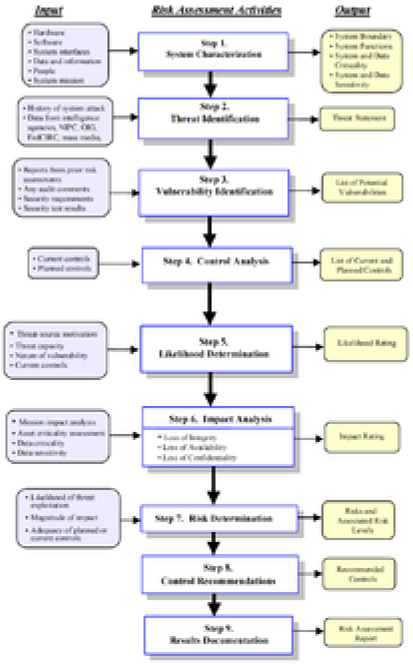


Figure 3-1. Risk Assessment Methodology Flowchart

Risk assessment according NIST SP 800-30 Figure 3-1

To determine the likelihood of a future adverse event, threats to an IT system must be in conjunction with the potential vulnerabilities and the controls in place for the IT system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of vulnerability. The level of impact is governed by the potential mission impacts and produces a relative value for the IT assets and resources affected (e.g., the criticality sensitivity of the IT system components and data). The risk assessment methodology encompasses nine primary steps:[7]

- Step 1 System Characterization
- Step 2 Threat Identification
- Step 3 Vulnerability Identification
- Step 4 Control Analysis
- Step 5 Likelihood Determination

- Step 6 Impact Analysis
- Step 7 Risk Determination
- Step 8 Control Recommendations
- Step 9 Results Documentation

Risk mitigation

Risk mitigation, the second process according to SP 800–30, the third according to ISO 27005 of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization's resources and mission.

ISO 27005 framework

The risk treatment process aim at selecting security measures to:

- reduce
- retain
- avoid
- transfer

risk and produce a risk treatment plan, that is the output of the process with the residual risks subject to the acceptance of management.

There are some list to select appropriate security measures,[13] but is up to the single organization to choose the most appropriate one according to its business strategy, constraints of the environment and circumstances. The choice should be rational and documented. The importance of accepting a risk that is too costly to reduce is very high and led to the fact that risk acceptance is considered a separate process.[12]

Risk transfer apply were the risk has a very high impact but is not easy to reduce significantly the likelihood by means of security controls: the insurance premium should be compared against the mitigation costs, eventually evaluating some mixed strategy to partially treat the risk. Another option is to outsource the risk to somebody more efficient to manage the risk.[19]

Risk avoidance describe any action where ways of conducting business are changed to avoid any risk occurrence. For example, the choice of not storing sensitive information about customers can be an avoidance for the risk that customer data can be stolen.

The *residual risks*, i.e. the risk remaining after risk treatment decision have been taken, should be estimated to ensure that sufficient protection is achieved. If the residual risk is unacceptable, the risk treatment process should be iterated.

NIST SP 800 30 framework

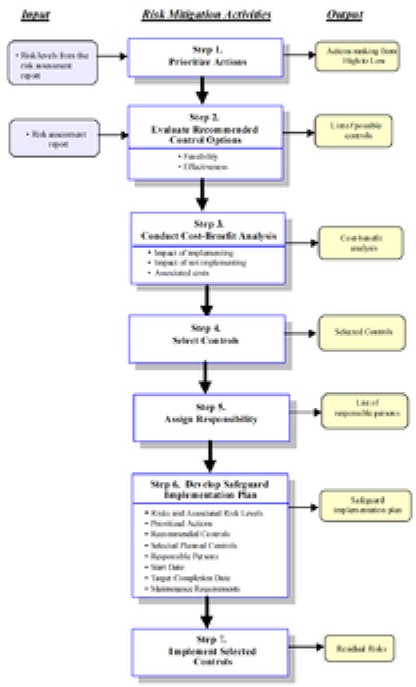

Input
Risk Mitigation Activities
Output
• Risk levels from the risk assessment report
Step 1. Prioritize Actions
Actions ranking from High to Low
• Risk assessment report
Step 2. Evaluate Recommended Control Options
• Feasibility
• Effectiveness
List of possible controls
Step 3. Conduct Cost-Benefit Analysis
• Impact of implementing
• Impact of not implementing
• Associated costs
Cost-benefit analysis
Step 4. Select Controls
Selected Controls
Step 5. Assign Responsibility
List of responsible persons
Step 6. Develop Safeguard Implementation Plan
• Risks and Associated Risk Levels
• Prioritized Actions
• Recommended Controls
• Selected Planned Controls
• Responsible Persons
• Start Date
• Target Completion Date
• Maintenance Requirements
Safeguard implementation plan
Step 7. Implement Selected Controls
Residual Risks

Figure 4-2. Risk Mitigation Methodology Flowchart

Risk mitigation methodology flow chart from NIST SP 800-30 Figure 4-2

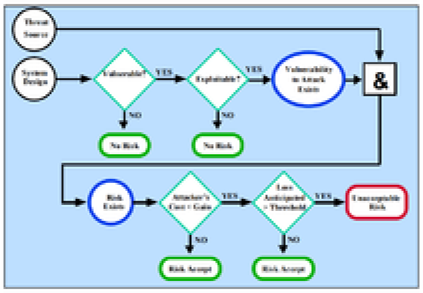


Figure 4-1. Risk Mitigation Action Points

Risk mitigation action point according to NIST SP 800-30 Figure 4-1

Risk mitigation is a systematic methodology used by senior management to reduce mission risk.[7]
Risk mitigation can be achieved through any of the following risk mitigation options:

- **Risk Assumption**. To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level
- **Risk Avoidance**. To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)
- **Risk Limitation**. To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)
- **Risk Planning**. To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls
- **Research and Acknowledgement**. To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability
- **Risk Transference**. To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

Address the greatest risks and strive for sufficient risk mitigation at the lowest cost, with minimal impact on other mission capabilities: this is the suggestion contained in[7]

Risk communication

Risk communication is a horizontal process that interacts bidirectionally with all other processes of risk management. Its purpose is to establish a common understanding of all aspect of risk among all the organization's stakeholder. Establishing a common understanding is important, since it influences decisions to be taken. The Risk Reduction Overview method [20] is specifically designed for this process. It presents a comprehensible overview of the coherence of risks, measures and residual risks to achieve this common understanding.

Risk monitoring and review

Risk management is an ongoing, never ending process. Within this process implemented security measures are regularly monitored and reviewed to ensure that they work as planned and that changes in the environment rendered them ineffective. Business requirements, vulnerabilities and threats can change over the time.

Regular audits should be scheduled and should be conducted by an independent party, i.e. somebody not under the control of whom is responsible for the implementations or daily management of ISMS.

IT evaluation and assessment

Security controls should be validated. Technical controls are possible complex systems that are to tested and verified. The hardest part to validate is people knowledge of procedural controls and the effectiveness of the real application in daily business of the security procedures.[7]

Vulnerability assessment, both internal and external, and Penetration test are instruments for verifying the status of security controls.

Information technology security audit is an organizational and procedural control with the aim of evaluating security. The IT systems of most organization are evolving quite rapidly. Risk management should cope with these changes through change authorization after risk re evaluation of the affected systems and processes and periodically review the risks and mitigation actions.[5]

Monitoring system events according to a security monitoring strategy, an incident response plan and security validation and metrics are fundamental activities to assure that an optimal level of security is obtained.
It is important to monitor the new vulnerabilities, apply procedural and technical security controls like regularly updating software, and evaluate other kinds of controls to deal with zero-day attacks.

The attitude of involved people to benchmark against best practice and follow the seminars of professional associations in the sector are factors to assure the state of art of an organization IT risk management practice.

Integrating risk management into system development life cycle

Effective risk management must be totally integrated into the SDLC. An IT system's SDLC has five phases: initiation, development or acquisition, implementation, operation or maintenance, and disposal. The risk management methodology is the same regardless of the SDLC phase for which the assessment is being conducted. Risk management is an iterative process that can be performed during each major phase of the SDLC.[7]

Table 2-1 Integration of Risk Management into the SDLC[7]

SDLC Phases	Phase Characteristics	Support from Risk Management Activities
Phase 1: Initiation	The need for an IT system is expressed and the purpose and scope of the IT system is documented	Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy)
Phase 2: Development or Acquisition	The IT system is designed, purchased, programmed, developed, or otherwise constructed	The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design tradeoffs during system development
Phase 3: Implementation	The system security features should be configured, enabled, tested, and verified	The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation
Phase 4: Operation or Maintenance	The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to	Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces)

	organizational processes, policies, and procedures	
Phase 5: Disposal	This phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software	Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner

NIST SP 800-64[21] is devoted to this topic.

Early integration of security in the SDLC enables agencies to maximize return on investment in their security programs, through:[21]

- Early identification and mitigation of security vulnerabilities and misconfigurations, resulting in lower cost of security control implementation and vulnerability mitigation;
- Awareness of potential engineering challenges caused by mandatory security controls;
- Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques; and
- Facilitation of informed executive decision making through comprehensive risk management in a timely manner.

This guide[21] focuses on the information security components of the SDLC. First, descriptions of the key security roles and responsibilities that are needed in most information system developments are provided. Second, sufficient information about the SDLC is provided to allow a person who is unfamiliar with the SDLC process to understand the relationship between information security and the SDLC. The document integrates the security steps into the linear, sequential (a.k.a. waterfall) SDLC. The five-step SDLC cited in the document is an example of one method of development and is not intended to mandate this methodology. Lastly, SP 800-64 provides insight into IT projects and initiatives that are not as clearly defined as SDLC-based developments, such as service-oriented architectures, cross-organization projects, and IT facility developments.

Security can be incorporated into information systems acquisition, development and maintenance by implementing effective security practices in the following areas.[22]

- Security requirements for information systems
- Correct processing in applications
- Cryptographic controls
- Security of system files
- Security in development and support processes
- Technical vulnerability management

Information systems security begins with incorporating security into the requirements process for any new application or system enhancement. Security should be designed into the system from the beginning. Security requirements are presented to the vendor during the requirements phase of a product purchase. Formal testing should be done to determine whether the product meets the required security specifications prior to purchasing the product.

Correct processing in applications is essential in order to prevent errors and to mitigate loss, unauthorized modification or misuse of information. Effective coding techniques include validating input and output data, protecting message integrity using encryption, checking for processing errors, and creating activity logs.

Applied properly, cryptographic controls provide effective mechanisms for protecting the confidentiality, authenticity and integrity of information. An institution should develop policies on the use of encryption, including proper key management. Disk Encryption is one way to protect data at rest. Data in transit can be protected from alteration and unauthorized viewing using SSL certificates issued through a Certificate Authority that has implemented a Public Key Infrastructure.

System files used by applications must be protected in order to ensure the integrity and stability of the application. Using source code repositories with version control, extensive testing, production back-off plans, and appropriate access to program code are some effective measures that can be used to protect an application's files.

Security in development and support processes is an essential part of a comprehensive quality assurance and production control process, and would usually involve training and continuous oversight by the most experienced staff.

Applications need to be monitored and patched for technical vulnerabilities. Procedures for applying patches should include evaluating the patches to determine their appropriateness, and whether or not they can be successfully removed in case of a negative impact.

Critique of risk management as a methodology

Risk management as a scientific methodology has been criticized as being shallow.[3] Major IT risk management programmes for large organizations, such as mandated by the US Federal Information Security Management Act, have been criticized.

By avoiding the complexity that accompanies the formal probabilistic model of risks and uncertainty, risk management looks more like a process that attempts to guess rather than formally predict the future on the basis of statistical evidence. It is highly subjective in assessing the value of assets, the likelihood of threats occurrence and the significance of the impact.

However, a better way to deal with the subject has not emerged.[3]

Risk managements methods

It is quite hard to list most of the methods that at least partially support the IT risk management process. Efforts in this direction were done by:

- NIST Description of Automated Risk Management Packages That NIST/NCSC Risk Management Research Laboratory Has Examined, updated 1991
- ENISA[23] in 2006; a list of methods and tools is available on line with a comparison engine.[24] Among them the most widely used are:[3]
    - CRAMM Developed by British government is compliant to ISO/IEC 17799, Gramm–Leach–Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA)
    - EBIOS developed by the French government it is compliant with major security standards: ISO/IEC 27001, ISO/IEC 13335, ISO/IEC 15408, ISO/IEC 17799 and ISO/IEC 21287
    - Standard of Good Practice developed by Information Security Forum (ISF)
    - Mehari developed by Clusif Club de la Sécurité de l'Information Français[25]

    - TIK IT Risk Framework developed by IT Risk Institute[26]
    - Octave developed by Carnegie Mellon University, SEI (Software Engineering Institute) The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE^{SM}) approach defines a risk-based strategic assessment and planning technique for security.
    - IT-Grundschutz (IT Baseline Protection Manual) developed by Federal Office for Information Security (BSI) (Germany); IT-Grundschutz provides a method for an organization to establish an Information Security Management System (ISMS). It comprises both generic IT security recommendations for establishing an applicable IT security process and detailed technical recommendations to achieve the necessary IT security level for a specific domain

Enisa report[2] classified the different methods regarding completeness, free availability, tool support; the result is that:

- EBIOS, ISF methods, IT-Grundschutz cover deeply all the aspects (Risk Identification, Risk analysis, Risk evaluation, Risk assessment, Risk treatment, Risk acceptance, Risk communication),
- EBIOS and IT-Grundschutz are the only ones freely available and
- only EBIOS has an open source tool to support it.

The Factor Analysis of Information Risk (FAIR) main document, "An Introduction to Factor Analysis of Information Risk (FAIR)", Risk Management Insight LLC, November 2006;[16] outline that most of the methods above lack of rigorous definition of risk and its factors. FAIR is not another methodology to deal with risk management, but it complements existing methodologies.[27]

FAIR has had a good acceptance, mainly by The Open Group and ISACA.

ISACA developed a methodology, called Risk IT, to address various kind of IT related risks, chiefly security related risks. It is integrated with COBIT, a general framework to manage IT. Risk IT has a broader concept of IT risk than other methodologies, it encompasses not just only the negative impact of operations and service delivery which can bring destruction or reduction of the value of the organization, but also the benefit\value enabling risk associated to missing opportunities to use technology to enable or enhance business or the IT project management for aspects like overspending or late delivery with adverse business impact.[1]

The "*Build Security In*" initiative of Homeland Security Department of United States, cites FAIR.[28] The initiative Build Security In is a collaborative effort that provides practices, tools, guidelines, rules, principles, and other resources that software developers, architects, and security practitioners can use to build security into software in every phase of its development. So it chiefly address Secure coding.

In 2016, Threat Sketch launched an abbreviated cyber security risk assessment specifically for small organizations.[29][30] The methodology uses real options to forecast and prioritize a fixed list of high-level threats.

In the US, data and privacy legislation continue to evolve to focus on **'reasonable security'** for sensitive information risk management. The goal is to ensure organizations establish their duty of care when it comes to managing data. Businesses are responsible to understand their risk posture to prevent foreseeable harm reasonable safeguards based on their specific working environment.

Standards

There are a number of standards about IT risk and IT risk management. For a description see the main article.

Laws

See also

Business and economics portal

- Access control
- Asset (computing)
- Asset management
- Assessment
- Attack (computing)
- Availability
- Benchmark

- Best practice
- Business continuity
- Business continuity plan
- Business process
- Chief information officer
- Chief information security officer
- COBIT
- Common Vulnerabilities and Exposures (CVE)
- Communications
- Computer insecurity
- Computer security
- Confidentiality
- COSO
- Countermeasure (computer)
- CRAMM
- Common Vulnerability Scoring System (CVSS)
- Decision theory
- EBIOS
- ENISA
- Enterprise risk management
- Environmental security
- Evaluation
- Exploit (computer security)
- Factor Analysis of Information Risk
- FISMA
- Full disclosure (computer security)

- Gramm–Leach–Bliley Act
- Health Insurance Portability and Accountability Act
- Homeland Security Department
- Human resources
- Incident management
- Information security
- Information Security Forum
- Information security management
- Information technology
- Information technology security audit
- Insurance
- Integrity
- ISACA
- ISO
- ISO/IEC 15408
- ISO/IEC 17799
- ISO/IEC 27000-series
- ISO/IEC 27001
- ISO/IEC 27005
- IT-Grundschutz
- IT risk
- Mehari
- Methodology
- National Information Assurance Training and Education Center
- National Security
- NIST

- Organization
- OWASP
- Patch (computing)
- Penetration test
- Physical security
- Privacy
- Regulatory compliance
- Risk
- Risk analysis (engineering)
- Risk appetite
- Risk assessment
- Risk factor (computing)
- Risk management
- Risk IT
- Risk register
- Secure coding
- Security control
- Security policy
- Security risk
- Security service (telecommunication)
- Standard of Good Practice
- Stakeholder (corporate)
- Systems Development Life Cycle
- The Open Group
- Threat
- Vulnerability

- Vulnerability assessment
- Vulnerability management
- w3af
- zero-day attack

References

1. *"ISACA THE RISK IT FRAMEWORK (registration required)" (http://www.isaca.org/Knowledge-Center/Research/Documents/RiskIT-FW-18Nov09-Research.pdf) (PDF).*
2. *Enisa Risk management, Risk assessment inventory, page 46 (https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools)*
3. *Katsicas, Sokratis K. (2009). "35". In Vacca, John (ed.). Computer and Information Security Handbook. Morgan Kaufmann Publications. Elsevier Inc. p. 605. ISBN 978-0-12-374354-1.*
4. *"Risk is a combination of the likelihood of an occurrence of a hazardous event or exposure(s) and the severity of injury or ill health that can be caused by the event or exposure(s)" (OHSAS 18001:2007).*
5. *Caballero, Albert (2009). "14". In Vacca, John (ed.). Computer and Information Security Handbook. Morgan Kaufmann Publications. Elsevier Inc. p. 232. ISBN 978-0-12-374354-1.*
6. *ISACA (2006). CISA Review Manual 2006 (http://www.isaca.org/) . Information Systems Audit and Control Association. p. 85. ISBN 978-1-933284-15-6.*
7. *Feringa, Alexis; Goguen, Alice; Stoneburner, Gary (1 July 2002). "Risk Management Guide for Information Technology Systems" (https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01) . doi:10.6028/NIST.SP.800-30 (https://doi.org/10.6028%2FNIST.SP.800-30) – via csrc.nist.gov.*
8. *"Glossary of Terms" (https://www.niatec.iri.isu.edu/Glossary.aspx?term=4253&alpha=R) . www.niatec.iri.isu.edu.*
9. *The Risk IT Framework by ISACA, ISBN 978-1-60420-111-6*
10. *The Risk IT Practitioner Guide, Appendix 3 ISACA (http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Practitioner-Guide.aspx) ISBN 978-1-60420-116-1* (registration *required)*
11. *Standard of Good Practice by Information Security Forum (ISF) Section SM3.4 Information risk analysis methodologies (https://www.isfsecuritystandard.com)*
12. *ISO/IEC, "Information technology -- Security techniques-Information security risk management" ISO/IEC FIDIS 27005:2008*
13. *ISO/IEC 27001*

14. *Official (ISC)2 Guide to CISSP CBK. Risk Management: Auerbach Publications. 2007. p. 1065.*

15. *"CNN article about a class action settlement for a Veteran Affair stolen laptop" (http://articles.cnn.com/2009-01-27/politics/va.data.theft_1_laptop-personal-data-single-veteran?_s=PM:POLITICS) .*

16. *"An Introduction to Factor Analysis of Information Risk" (FAIR), Risk Management Insight LLC, November 2006 (http://www.riskmanagementinsight.com/media/docs/FAIR_introduction.pdf) Archived (https://web.archive.org/web/20141118061526/http://www.riskmanagementinsight.com/media/docs/FAIR_introduction.pdf) 2014-11-18 at the Wayback Machine;*

17. *Spring, J.; Kern, S.; Summers, A. (2015-05-01). "Global adversarial capability modeling". 2015 APWG Symposium on Electronic Crime Research (ECrime): 1–21. doi:10.1109/ECRIME.2015.7120797 (https://doi.org/10.1109%2FECRIME.2015.7120797) . ISBN 978-1-4799-8909-6. S2CID 24580989 (https://api.semanticscholar.org/CorpusID:24580989) .*

18. *British Standard Institute "ISMSs-Part 3: Guidelines for information security risk management" BS 7799-3:2006*

19. *Costas Lambrinoudakisa, Stefanos Gritzalisa, Petros Hatzopoulosb, Athanasios N. Yannacopoulosb, Sokratis Katsikasa, "A formal model for pricing information systems insurance contracts", Computer Standards & Interfaces - Volume 27, Issue 5, June 2005, Pages 521-532 doi:10.1016/j.csi.2005.01.010 (https://doi.org/10.1016%2Fj.csi.2005.01.010)*

20. *"Risk Reduction Overview" (http://rro.sourceforge.net/) . rro.sourceforge.net.*

21. *Gulick, Jessica; Fahlsing, Jim; Rossman, Hart; Scholl, Matthew; Stine, Kevin; Kissel, Richard (16 October 2008). "Security Considerations in the System Development Life Cycle" (https://csrc.nist.gov/publications/detail/sp/800-64/rev-2/final) . doi:10.6028/NIST.SP.800-64r2 (https://doi.org/10.6028%2FNIST.SP.800-64r2) – via csrc.nist.gov.*

22. *"Wiki Content Now Available at Spaces" (https://wiki.internet2.edu/index.html) . wiki.internet2.edu.*

23. *"Inventory of Risk Management / Risk Assessment Methods" (https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/inventory-of-risk-management-risk-assessment-methods-1) . www.enisa.europa.eu.*

24. *"Inventory of Risk Management / Risk Assessment Methods and Tools" (https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/inventory-of-risk-management-risk-assessment-methods-and-tools) . www.enisa.europa.eu.*

25. *"CLUSIF | Bienvenue" (https://web.archive.org/web/20101026162937/http://www.clusif.asso.fr/) . Archived from the original (https://www.clusif.asso.fr/) on 2010-10-26. Retrieved 2010-12-14.*

26. *http://itriskinstitute.com/*

27. *Technical Standard Risk Taxonomy ISBN 1-931624-77-1 Document Number: C081 Published by The Open Group, January 2009.*

28. *"Build Security In - US-CERT" (https://www.us-cert.gov/bsi) . www.us-cert.gov.*

29. *"Threat Sketch: A Start-up Grows Up in the Innovation Quarter" (http://hub.innovationquarter.com/2016/10/05/a-start-up-grows-up-in-the-innovation-quarter/) . Innovation Quarter Hub. 2016-10-05. Retrieved 2016-11-15.*

30. *"Triad Entrepreneurs Share Business Ideas on Startup Weekend" (http://www.twcnews.com/nc/triad/news/2016/11/11/entrepreneurs-share-business-ideas-on-startup-weekend.html) . TWC News. Retrieved 2016-11-15.*

External links

Wikimedia Commons has media related to ***IT risk management***.

- Internet2 Information Security Guide: Effective Practices and Solutions for Higher Education (https://wiki.internet2.edu/confluence/display/itsg2/Home)
- Risk Management - Principles and Inventories for Risk Management / Risk Assessment methods and tools (http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/files/deliverables/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools/at_download/fullReport) , Publication date: Jun 01, 2006 Authors:Conducted by the Technical Department of ENISA Section Risk Management
- Clusif Club de la Sécurité de l'Information Français (https://web.archive.org/web/20101026162937/http://www.clusif.asso.fr/)
- 800-30 NIST Risk Management Guide (http://csrc.nist.gov/publications/PubsSPs.html#800-30)
- 800-39 NIST DRAFT Managing Risk from Information Systems: An Organizational Perspective (http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-39)
- FIPS Publication 199, Standards for Security Categorization of Federal Information and Information (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)
- FIPS Publication 200 Minimum Security Requirements for Federal Information and Information Systems (http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf)
- 800-37 NIST Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf)

- FISMApedia is a collection of documents and discussions focused on USA Federal IT security (http://fismapedia.org/index.php?title=Main_Page)
- Anderson, K. "Intelligence-Based Threat Assessments for Information Networks and Infrastructures: A White Paper (https://web.archive.org/web/20110519015050/http://www.aracnet.com/~kea/Papers/threat_white_paper.pdf) ", 2005.
- Danny Lieberman, "Using a Practical Threat Modeling Quantitative Approach for data security (http://www.software.co.il/case-studies/254-data-security-threat-assessment.html) ", 2009

Retrieved from "https://en.wikipedia.org/w/index.php?title=IT_risk_management&oldid=1115761874"