Assessing Information Security Risk Management in Organizations

Prof. Mohamed M. El Hadi
Sadat Academy for
Management Sciences

ABSTRACT

Information security risks are those risks that arise from the loss of confidentiality, integrity or availability of information or information systems and reflect the potential adverse impacts to organizational operations (i.e., goal, mission, functions, image and reputation), organizational assets, personnel, other organizations, and the country as a whole. Risk assessment is the process of identifying, estimating, and prioritizing information security risks. Assessing risk requires the useful analysis of threat and vulnerabilities information to determine the extent to which events or circumstances could adversely impact on organization/institution and the likelihood that such events or circumstances will occur.

This technical paper describes the fundamental concepts and processes related with assessing information security risk management within organizations/institutions including: (1) a high level overview of the risk management process and risk assessment, (2) the basic concepts used in conducting risk assessments, and (3) how risk assessments can be applied across the organization's risk management three hierarchical Tiers including Tier 1 and Tier 3 of the information systems within any organization. Therefore, this work identifies and explains the main themes regarding risk assessments in organizations: Risk management process and its main four components regarding assessing, framing, monitoring and responding; Risk assessment as the main component that addresses the potential adverse impacts on organizational operations, assets, etc.; Key risk assessment concepts that indicate risk models (threats, vulnerabilities and predisposing conditions, etc.), assessment approaches concerned with quantitative and semi-quantitative assessments as well as qualitative assessment, and analysis approaches andeffects of organizational culture on risk assessment; Applications of risk assessments through the main three risk assessments hierarchy's Tiers; Risk management process with its main four steps or operations as well as the risk management framework; Finally the administrative, proce4dural and technical controls conforming the policy and controlling the risks.

Keywords: Information Security, Risk Assessment, Risk Analysis, Risk Management Process, Risk Management Framework, Risk Models, Threats, Vulnerabilities, Predisposing Conditions.

1. Introduction:

Organizations/ institutions (that describes an entity of any size, complexity or positioning within an organizational structure that is charged with carrying out assigned mission/business processes and uses information systems in support of those processes)whether they are in public, private or governmental sectors depend on information technology in the form of common infrastructure sets of shared services and sets of common controls, as well asinformation systems or discrete information resources organized for collecting, processing, storing, maintaining, using, sharing, disseminating, and/or disposing of information to successfully carry out the organizations/institutions' missions an business functions.

Information systems can include very diverse entries ranging from office networks, financial and personnel systems to very specialized systems (e.g. industrial process control systems, telecommunications systems, environmental control systems, etc.). Information systems are subject to serious threats that can have adverse effects on organizational operations and assets, human resources, other organizations/institutions, as well as on the country itself by exploiting known and un-known vulnerabilities to compromise the confidentiality, integrity or availability of the information being processed, stored, or transmitted by these systems.

Threats to information systems can include purposeful attacks, environmental disruptions, human/machine errors, and structural failures, and can result in harm to national and economic security interests of the country.

Thereafter, it is imperative that the organizations' managers at all levels understand their responsibilities and are being accountable for managing information security risk, i.e. the risk related with the operation and use of information systems that support the goals, missions, and business functions of their organizations.

Risk assessment is considered one of the fundamental components of an institutional or organizational risk management process. Risk assessments are used to identify, estimate and prioritize risk to organization operations (i.e. goals, missions, functions, image and reputation), organizational assets, personnel and other organizations as well as the country itself resulting from the operation and use of information system. The purpose of risk assessments is to inform organization's decision makers and support risk responses by identifying the followings:

1. Related threats to organizations or threats directed through organizations against other organizations.

2. Vulnerabilities both internal and external for organizations.

3. Harmful impact to organizations that may occur given the potential for threats exploiting vulnerabilities.

4. Likelihood that harmful impact will occur.

The end result is a determination of risk, i.e. typically a function of the degree of harm and likelihood of hierarchy including Tier 1 (organizational level), Tier 2 (goal, mission/business process level), and Tier 3 (information system level). At Tiers 1 and 2, organizations use risk assessments to evaluate, for example, systematic information security-related risks associated with organizational governance and management activities, mission/business processes, organization architecture, or the funding of information security program. At Tier 3, organizations use risk assessments to more effectively support the implementation of Risk Management Framework (i.e. security organizations, security control selection, implementation and assessment, information system and common control authorization, and security control monitoring.

2. Risk Management Process:

To identify and make good business decisions about privacy and security requirements, any individual or organization must perform security risk assessments, privacy risk assessments and business risk assessments. This must be done on an ongoing basis, as the individual or organization that IT exists in an environment which is constantly identifying new issues and risks, but not limited to security domain. In particular security risk requirements are required.

It is important to understand the business relevance to risks identified, how much risk is acceptable, what types of risk may arise from new technologies, and how much to spend on mitigating risk.

A through risk assessment includes different types of risks, including IT security, privacy, safety, loss of access to IT-based services and data resources, corporate risks, and human error factors. This enables risks to be considered when determining technology strategies and tactics.

Therefore, risk management provides a cohesive vision to prevent unwise investment in security, privacy or other technologies based on popular demand, sales presentations, and sensationalist press report. It is about much more than keeping hackers from stealing personal individual or organizational information. Rather, it is critical to address such issues as:

- Protecting confidentiality of personal, organizational or the country information resources,
- Legal compliance,
- Safe provision of information required, Avoiding any functional error, and
- The cost and benefit of protecting measures.

While the majority of risks can have negative impacts, risk analysis can expose opportunities to enhance the quality of the offered service, and reducing conflicts through automated checks against a database. Efficient risk management enables top and middle managers, as well as technical and operational staff to:

- Improve business performance by information and improving decision making and planning,
- Promote a more innovative, less risk reverse culture in which the taking of calculated risk is pursuit of opportunities is encouraged,
- Provide a sound basis for integrated risk management and internal control as components of good corporate or national governance,
- Assist in meeting the needed service requirements and objectives,
- Facilitate partnerships with other individuals, organizations or the Nation as a whole to address the issues

inherent in interoperable systems and data sharing,

- Benefit individuals, organizations or countries who often receive needed information from multiple providers by effective information sharing to improve the safety and quality of information and services.

Risk management is a fundamental process, which include: framing risk, assessing risk, responding to risk, and monitoring risk.

The following Figure illustrates the above stated four steps in risk management process, including the risk assessment step and the information and communications flows necessary to make the process work effectively:

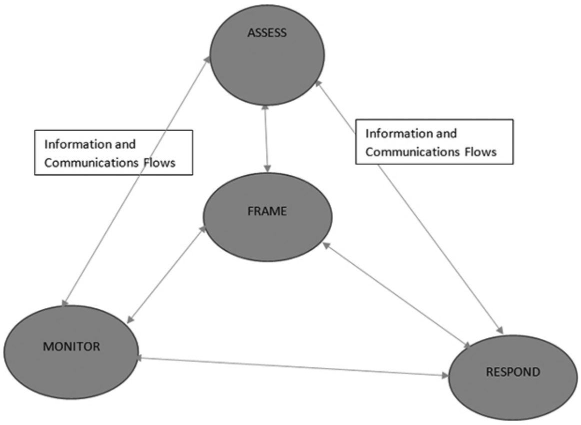
ASSESS
Information and Communications Flows
Information and Communications Flows
FRAME
MONITOR
RESPOND

Fig. 1 Risk Assessment within Risk Management Process

As shown in the above figure, the first component of the risk management addresses how

Organizations or institutions frame or establish a risk context that is describing the environment in which risk-based descriptions are made. The purpose of the risk framing component is to produce risk management strategy that addresses how organizations intend to assess risk, respond to risk and monitor risk, making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions. The risk management strategy establishes a foundation for managing risk and delineates the boundaries risk-based decisions within organizations. In the absence of an explicit or formal organizational risk management strategy, organizational resources (e.g., tools, data repositories) and references (e.g., exemplary risk assessment reports) can be used to discern those aspects of the organization›s approach to risk management that affect risk assessment.

The 2nd component of risk management addresses how organizations assess risk within the context of the organizational risk frame. The purpose of risk assessment component is to identify the followings:

1. Threats to organizations/institutions,

2. Vulnerabilities internal and external to organizations/institutions,

3. The harm (i.e., adverse impact) that may occur given the potential for threats exploring vulnerabilities,

4. The likelihood that harm will occur.

The end result is a determination of risk.

The 3rd component of risk management addresses how organizations/institutions, respond to risk once that risk is determined-based on the result of a risk assessment. The purpose of risk response component is to provide a consistent organizational-wide response to risk in accordance with the organizational risk frame by the followings:

1. Developing alternative courses of action for responding risk,

2. Evaluating the alternative course of action,

3. Organizations/institutions, Determining appropriate courses of action consistent with organizational risk tolerance, and

4. Implementing risk responses based on selected courses of action.

The 4th component of risk management addresses how organizations/institutions monitor risk over time. The purpose of risk monitoring component is to:

1. Determine the ongoing effectiveness of risk responses (consisted with the organizational risk frame),

2. Identify risk-impacting changes to organizational information systems and environments in which the system operates), and\

3. Verify that planned risk responses are in implemented and information security requirements derive from the traceable to organizational goal, missions/ business functions, legislations, directives, regulations, policies, standards and guidelines are being satisfied.

1. Risk Assessment:

The risk assessment as a main component of risk management provides a step-by-step process for organizations/institutions on the followings:

1. How to prepare for risk assessments?

2. How to conduct risk assessments?

3. How to communicate risk assessment results to key organizational personnel?

4. How to maintain the risk assessments over time?

Risk assessments are not simply one-time activities that provide permanent and definitive information for decision makers to guide and inform responses to information security risks.

Risk assessments address the potential adverse impacts to organizational operations and assets, personnel, other organizations/institutions, and economic and national security that is of interests to many countries in the world, arising from the operation and use of information systems and information processed, stored and transmitted by those systems. Organizations/institutions conduct risk assessment to determine risks that are common to the organization›s core goals, mission, business functions, processes, business segments, common infrastructure support service, or information systems. Risk assessments can support a wide-variety of risk-based decisions and activities by organizational officials across all the three Tiers in risk management hierarchy including, but not limited to the followings:

• Development of an information security architecture,

• Definition of interconnection requirements for information systems (including systems supporting, goals, mission/business processes and common infrastructure/support services),

• Design for security solutions for information systems and environments of operation including selection of security controls, information technology products, suppliers/supply chain) and contractors,

• Authorization (or denial of authorization) to operate information systems or to use security controls inherited by those systems (i.e., common controls),

• Modification of goals, missions/business functions and/or goal, mission/business processes permanently, or for a specific time frame (e.g., until a newly discovered threat or vulnerability is addressed,

• Implementation of security solutions (e.g., whether information technology products or configurations for those products that meet established requirements), and

• Operation and maintenance of security solutions (e.g., continuous monitoring, strategies and programs ongoing authorizations).

Because organizational goals, missions and business functions, supporting mission/business processes, information systems, threats, vulnerabilities and environments of operation that tend to change over time, the validity, and usefulness of any risk assessment that is bounded.

4. KeyRisk Concepts:

Risk is a measure of extent to which an entity is threatened by a practical circumstance or event, and is typically a function of:

• The adverse impacts that would arise if the circumstance or event occurs, and

• The likelihood of occurrence.

Information security risks are those risks that arise from the loss of confidentiality, integrity or availability of information or information systems and reflect the potential adverse impacts to organizational operations (i.e., goal, mission, functions, image and reputation), organizational assets, personnel, other organizations, and the country as a whole. Risk assessment is the process of identifying, estimating, and prioritizing information security risks. Assessing risk requires the useful analysis of threat and vulnerabilities information to determine the extent to which events or circumstances could adversely impact on organization/institution and the likelihood that such events or circumstances will occur.

A typically risk assessment methodology includes the followings:

• A risk assessment process,

• An explicit risk model, defining key terms and assessable risk factors and thread relationships among factors,

• An assessment approach (e.g., quantitative, qualitative, or semi-qualitative), specifying the range of values those risk factors can assume during the risk assessment and how combinations of risk factors are identified, analyzed so that values of those factors can be fundamentally combined to evaluate risk, and

• An analysis approach (e.g., threat-oriented, asset/impact-oriented, or vulnerabilities-oriented).

Assessing how combinations of risk factors are identified, analyzed to ensure adequate coverage of the problem space at a consistent level of detail. Risk assessment methodologies are defined by the organizations and are a component of risk management strategy developed during the risk framing step of risk management process. The risk assessment methodologies are influenced in large measure by organizational risk management strategy. However, risk assessment methodologies can be customized for each risk assessment based on the purpose and scope of the assessment and the specific inputs organizations choose to make regarding the risk assessment process, risk model, assessment approach, and analysis approach.

The following figure indicates the fundamental components in the organizational risk frames and relationships among those components.

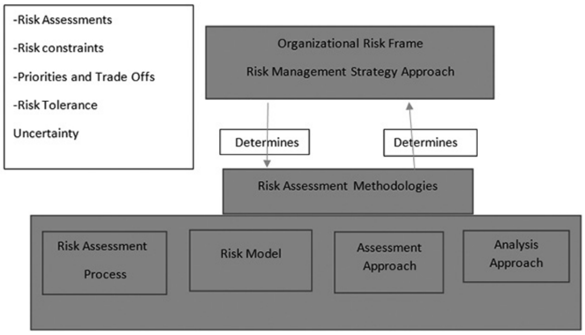

Fig. 2: Relationships among Risk Framing Components

Organizations/institutions can use a single risk assessment methodology or can employ multiple assessment methodologies, with the selection of a specific methodology depending on, for example:

1. The time frame for investment planning or for planning policy change,

2. The complexity/maturity of organizational mission/business processes (by organization architecture segment),

3. The phase of information systems in system development life cycle, or

4. The sensitivity of the information and information systems supporting the core of organizational mission/business functions.

By making explicit the risk model, the assessment approach, and analysis approach employed, and requiring a part of the assessment process, a rationale for the assessed values of risk factors, organizations can increase the reproducibility and repeatability of risk assessments. Reproducibility refer to the ability of different specialists/experts to produce the same results from the same data. Repeatabilityrefers to the ability to repeat the assessment in the future, in a manner that is consistent with and hence comparable to prior assessments, enabling the organization to identify trends.

4.1 Risk Models:

Risk models define the risk factors to be assessed and the relationships among those factors. The documentation of the model includes:

• Identification of risk factors (definitions, descriptions, value scale), and

• Identification of relationships among those factors (both conceptual relationships, presented descriptively, and algorithms for combining values).

Risk factors are the characteristics used in the risk model as inputs to determining levels in risk assessments. Risk factors are also used extensively in the risk communications to highlight what strongly affects the levels of risk in particular situations, circumstances or contexts. Typical risk factors include threat, vulnerabilities, impact, likelihood, and predisposing condition. Risk factors can be decomposed into more detailed characteristics (e.g., threats decomposed into threat sources and threat events). A risk factor can have a single assessable characteristics (e.g., impact severity) or multiple characteristics, some of which not be assessable. Characteristics which are not assessable typically help determine what lower-level characteristics are relevant. For example, a threat source has a characteristic threat type (using a taxonomy of threat types, which are nominal rather than assessable). The threat type determines which of the more detailed characteristics are relevant(e.g., a threat source of type adversary has associated characteristic, of capabilities, intent, and targeting, which are directly assessable characteristics).

4.1.1Threats: A threat is any event or circumstance with the potential to adversary impact organizational operations and assets, personnel. Other organizations, or the country through an information system via unauthorized access, destruction, disclosure, or modification of information and/or denial of service. Organization can choose to specify threat events as:

-Single events, actions, or circumstances, or

-Sets and/or sequences of related actions, activities, and/or circumstances.

Threat events are caused by threat sources. A threat source is characterized as:

-The intent and method targeted at the exploitation of a vulnerability, and

-A situation and method that may accidently exploit a vulnerability.

In general, types of threat sources include the followings:

1. Hostile cyber or physical attacks,

2. Human errors of omission or commission,

3. Structural failures of organization-controlled resource (hardware, software, environmental controls), and

4. Natural and man-made disasters, accidents, and failure beyond, control of the organization.

Various taxonomies of threat sources have been developed. Some taxonomies of threat sources use the type of adverse impacts as an organizing principle. Multiple threat sources can initiate or cause the same threat event, for example, a provisioning server can be taken off-line by a denial-of-service attack, a deliberate act by malicious system administrator, an administrative error, a hardware fault, or a power failure.

Risk models differ in the degree of detail and complexity with which threat events are identified. When threat events are identified with great specificity, threat scenarios can be modeled, developed and analyzed. A threat scenarios is a set of discrete threat events, attributed to a specific source or multiple threat sources, ordered in time, that result in adverse effects. Threat events for cyber or physical attacks are characterized by the tactics, techniques, and procedures employed by adversaries.

Threat shifting is the response of adversaries to perceive safeguards and/or counter measures (i.e., security controls), in which adversaries change some characteristics of their intent/targeting in order to avoid and/or overcome those safeguards counter measures. Threat shifting can occur in one or more domains including:

1. The time domain (e.g., a delay in an attack or illegal entry to conduct additional surveillance),

2. The target domain (e.g., selecting a different target that is not well protected).

3. The resource domain (e.g., adding resources to the attack in order to reduce uncertainty or overcome safeguards and/or counter measures), or

4. The attack planning/attack method domain(e.g., changing the attack harm or attack path).

Threat shifting is a mutual consequence of a dynamic set of organizations between threat sources and types of organizational assets targeted.

Therefore, there are common threats for all Information Technology Systems:

- Information and data which is based on claims,

- Personnel identify threat is the misuse of another individual's identification, such as name, date of birth, ID No., insurance policy No., or bank account No.

- Failure of an IT system to receive the right data for any user/customer, etc.

- Presenting data for the wrong individual,

- Allowing un-detected changes to data, or

- Not being able to retrieve data due to outages can result in serious function errors that harm individuals. In particular, wireless devices, and networks - both WIFI and cellar ‑ are vulnerable to outages and low signal strength as well as deliberate denial of service attacks,

- Consumers' privacy-protective behaviors are a significant threats to individuals and organizations, as they may withhold relevant data if they believe their privacy is not respected. However, establishing stringent privacy controls ahead of offering a service especially in emergent situations, may produce similarly harmful results.

4.1.2Vulnerabilities and Predisposing Conditions: A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited a threat source.

The security of a vulnerability is an assessment of the relative importance of mitigating/remediating the vulnerability. The severity can be determined by the extent of the potential adverse impact if such a vulnerability is exploited by a threat source. Thus, the severity of vulnerabilities, in general, is context dependent. Most information systems vulnerabilities can be associated with security controls that either have not been applied (either intentionally or unintentionally), or have been applied, but retain some weaknesses.

Vulnerabilities are not identified only within information systems. Viewing information systems in a broader context, vulnerabilities can be found in organizational governance structure (e.g., the lack of effective risk management strategies and adequate risk framing for intra-organization communications), organization decisions about relative priorities of missions/business functions, or misalignment of organization architecture to support mission/business activities. Vulnerabilities can also be found in external relationships (e.g., dependencies on particular energy sources, supply chains, information technologies, and telecommunications providers), mission/business processes (e.g., poorly defined processes or processes that are not risk aware), and organization information security architecture (e.g., poor architectural decisions resulting in lack of diversity or residency in organizational information systems).

A predisposing condition is a condition that exists within an organization, a mission or business process, organization architecture. Information system, or environment of operation, which affects (i.e., increase or decrease) the likelihood that threat events, once initiated, result in adverse impacts to organizational operations and assets, personnel, other organizations, or the country as a whole. The concept of predisposing condition is also related to terms susceptibility or exposure. Organizations are not susceptible to risk (or exposed to risk) if a threat cannot exploit a vulnerabilities to cause adverse impact).

4.1.3Likelihood: The likelihood of occurrence is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities). The likelihood risk factor can combines an estimate of the likelihood that the threat event will be initiated with an estimate likelihood of impact. For adversarial threats, an assessment of likelihood of occurrence is typically based on:

- Adversary intent,

- Adversary capability, and

- Adversary targeting.

For other than adversarial threat events, the likelihood of occurrence is estimated using historical evidence, empirical data, or other factors. The likelihood of impact addresses the probability (or possibility) that the threat event will result in an adverse impact, regardless of the magnitude of harm that can be expected.

4.1.4Impact: The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. Such harm can be experienced by a variety of organizational and non-organizational stakeholders, including for example heads of organizations, mission and business owners, or individuals or groups in the public, private or government sectors relying on the organization, in essence, anyone with a vested interest in organization's operations, assets, or personnel including other organizations in partnership with the organization, or the country. The term organizational assets can have a very wide scope of applicability to include for example, high-impact programs, physical plant, mission-critical information systems, personnel, equipment, or a logically related group of systems, more broadly, organizational assets represent any resource or set of resources which the organization values, including intangible assets such as image or reputation.

Therefore, organizations make explicit the followings:

1. The process used to conduct impact determinations,

2. Assumptions related to impact determinations,

3. Sources and methods for obtaining impact information, and

4. The rationale for conclusions reached with regard to impact determinations.

4.1.5Risk: The following figure shows an example of a risk model including the key risk factors discussed above and the relationship among the factors. Each of the risk factors is used in the risk assessment process:

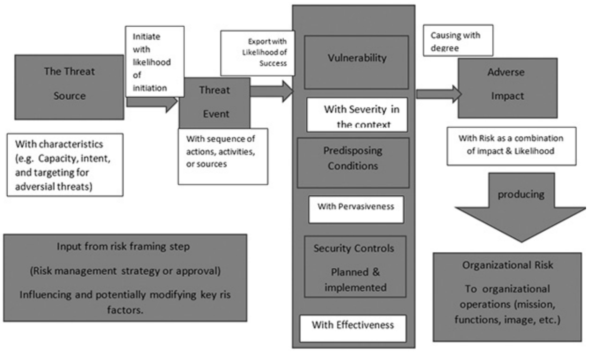
The Threat Source
Initiate with likelihood of initiation
Threat Event
Export with Likelihood of Success
Vulnerability
With Severity in the context
Predisposing Conditions
With Pervasiveness
Security Controls Planned & implemented
With Effectiveness
Causing with degree
Adverse Impact
With Risk as a combination of impact & Likelihood
producing
Organizational Risk
To organizational operations (mission, functions, image, etc.)
With characteristics (e.g. Capacity, intent, and targeting for adversial threats)
With sequence of actions, activities, or sources
Input from risk framing step
(Risk management strategy or approval)
Influencing and potentially modifying key ris factors.

Fig. 3: Generic Risk Model with Key Risk Factors

Therefore, as noted above, risk is a function of the likelihood of threat event's occurrence and potential adverse impact should the event occur. This definition accommodates many types of adverse impacts at all tiers in the risk management hierarchy (e.g., damage to image or reputation of the organization or financial loss at Tier 1: inability to successfully execute a specific mission, business process at Tier 2; or the resources expanded in responding to an information system incident at Tier 3). It also accommodates relationships among impacts (e.g., loss of current or future mission, business effectiveness due to the loss of data confidentiality; loss of confidence in critical information due to loss of data or system integrity; or unavailability or degradation of information or information systems). This broad definition also allows risk to be represented as a single value or as a vector (i.e., multiple values), in which different types of impacts are assessed separately. For the purpose of risk communication, risk is generally grouped according to the types of adverse impacts (and possibly the time frames in which those impacts are likely to be experienced).

4.1.6Aggregation: Organizations may use risk aggregation to roll up several discrete or lower level risks into a more general or higher level risk. Therefore, organizations may also use risk aggregation to efficiently manage the scope and scale of risk assessments involving multiple information systems and multiple missions, business processes with specified relationships and dependencies among those systems and processes. Risk aggregation, conducted primarily at Tier 1 and Tier 2 and occasionally at Tier 3, assesses the overall risk to organizational operations, assets, and individuals given the set of discrete risks. The discrete risks (e.g., the risk associated with a single information system supporting a well-defined mission/business process), the worst-case impact establishes an upper bound for the overall risk to organizational operations, assets, and individuals.

When aggregation risk, organizations consider the relationship among various discrete risks. For example, there may be a cause and effect relationship in that if one risk materials, another risk is more or less likely to materialize.

4.1.7Uncertainty: Uncertainty is inherent in the evaluation of risk, due to each considerations as:

1. Limitations on the extent to which the future will resemble the past,

2. Imperfect or incomplete knowledge of the threat (e.g., characteristics of adversaries

Including tactics, technique, and procedure),

3. Undiscovered vulnerabilities in technologies or products, and

4. Unrecognized dependencies, which can lead to unforeseen impacts.

Uncertainty about the value of specific risk factors can also be due to the step in risk management framework or phrase in the system development life cycle at which a risk assessment is performed. For example, at early phases in the system development life cycle, the presence and effectiveness of security controls may be unknown, while at later phases in the life cycle, the cost of evaluating control effectiveness may outweigh the benefits in terms of more fully informed decision making. Finally, uncertainty can be due to incomplete knowledge of risks associated with other information systems, missions, business processes, services, common infrastructures, and/or organizations. The reasons, can be communicated in the form of the results (e.g., by expressing results qualitatively, by providing ranges of values rather than single value for identified risks, or by using a visual representations of fuzzy regions rather than points).

4.2Assessment Approaches:

Risk, and its contributing factors, can be assessed in a variety of ways, including quantitatively, qualitatively, or semi-quantitatively of each risk assessment approach that is considered by organizations of having advantages and/or disadvantages. A preferred approach (or situation specific set of approaches) can be selected based on organizational culture and, in particular, attitudes toward the concepts of uncertainty and risk communication.

Quantitative assessments typically employ a set of methods, principles, or rules for assessing risk based on the use of numbers of risks, where the meaning and proportionally of values are maintained inside and outside the context of the assessment. This type of assessment most effectively supports cost-benefit analysis of alternative risk responses or causes of action. However, the meaning of qualitative results may not always be clear and may require interpretation and explanation, particularly to explain the assumptions and constraints on using the results. For example, organizations may typically ask if the numbers or results obtained in the risk assessments are reliable or if the differences in the obtained values are meaningful or insignificant.

In contrast of quantitative assessments,qualitative assessments typically employ a set of methods, principles, or rules for assessing risk based on non-numerical categories or levels (e.g., very low, low, moderate, high, very high). This type of assessment supports communicating risk results to decision makers. However, the range of values in qualitative assessments is comparatively small in most cases, making the relative prioritization or comparison within the set of supported risks difficulties. Additionally, unless each value is very clearly defined or is characterized by meaningful examples, different experts relying on their individual experiences could produce significant different assessment results. The repeatability and reproducibility of qualitative assessments are increased by annotation of assessed values (e.g., this value is high because of the following reasons) and by the use of tables or other well-defined functions to combine qualitative values.

The semi-quantitative assessments typically employ a set of methods, principles, or rules for assessing risk that uses bins, scales, or representative numbers whose values and meanings are not maintained in other contexts. This type of assessment can provide the benefits of quantitative and qualitative assessments. The bins (e.g., 0-15, 16-35, 36-70, 71-85, 86-100), or scale (e.g., 1-10) translate easily into qualitative terms that support risk communications for decision makers (e.g., a score of 95 can be interpreted as very high), while also allowing relative comparisons between values

In different bins or even within the same bin (e.g., the difference between risks scored 36 and 70 is relatively significant). The role of expert judgment in assessing values is more evident than in a purely qualitative approach.

4.3Analysis Approaches:

Analysis approaches differ with respect to the orientation or starting point of the risk assessment, level of detail in the assessment, and how risks due to similar threat scenarios are treated. An analysis approach can be: thereat-oriented, asses/impact-oriented, or vulnerability-oriented.

A threat-oriented approach starts with the identification of threat sources and threat events, and focuses on the development of threat scenarios; vulnerabilities are identified in context of threats, and for adversarial threats, impacts are identified on adversary intent. And asset/impact-oriented approach starts with the identification of impacts or consequences of concern and critical assets, possibly using the results of a mission or business impact analyses and identifying threat events that could lead to and/or threat sources that could seek those impacts or consequences. A vulnerability-oriented approach starts with a set of predisposing conditions or exploitable weaknesses, deficiencies in organizational information systems or the environments in which the systems operate, and identifies threat events that could exercise those vulnerabilities together with possible consequences of vulnerabilities being exercised.

Each analysis approach takes into consideration the same risk factors, and thus entail the same set of risk assessment activities, albeit in different order. Differences in the starting point of risk assessment6 can potentially bias the results, causing some risks not to be identified. Therefore, identification of risks from the second orientation (e.g., complementing a threat-oriented analysis approach with an asset/impact-oriented analysis approach) can improve the rigor and effectiveness of the analysis.

In addition to the orientation of the analysis approach, organizations can apply more rigorous analysis techniques (e.g., graph-based analyses) to provide an effective way to account for the many-to-many relationships between the followings:

- Threat sources and threat events (e.g., single threat event can be caused by multiple threat events),
- Threat events and vulnerabilities (i.e., a single threat event can exploit multiple vulnerabilities on a single vulnerability can be exploited by multiple threat events), and
- Threat events and impacts/assets (i.e., a single threat event can affect multi assets or have multiple impacts, and a single asset can be affected by threat events).

Rigorous analysis approaches also provide a way to account for whether, in the time frame for which risks are assessed, a specific adverse impact could occur (or a specific asset could be harmed) at most once, or perhaps repeatedly, depending on the nature of the impacts.

The objective of risk analysis is to identify and assess the risks to which the information system and its assets are exposed in order to select appropriate and justified security safeguards. There are five stages in risk analysis, which are:

1. Assess identification and valuation,
2. Threats assessment,
3. Vulnerabilities assessment,
4. Existed planned safeguards assessments, and
5. Risk assessment.

4.5 Effects of Organizational Culture on Risk Assessment:

Organizations can differ in the risk models, assessment approaches, and analysis approaches that they prefer for a variety of reasons. For example, culture issues can predisposing organizations to employ risk models that assume a constant value for one or most possible risk factors, so that some factors that are present in other organization's models are not represented. Culture can also predispose organizations to employ risk models that require detailed analyses using quantitative approaches. Alternately, organizations may prefer qualitative or semi-quantitative assessment approaches. In addition to differences among organizations, differences can also exist within organizations. Organizational risk frame, determine which risk models, assessment approaches, and analysis approaches to use under varying circumstances.

5. Application of Risk Assessments:

As stated previously, risk assessment can be conducted at all three tiers in the risk management hierarchy, organizational level, mission/business process level, and information system level.

The following figure illustrates the risk management hierarchy which provides multiple risk perspective from the strategic level to the tactical level. Traditional risk assessments generally faces at Tier 3 level (i.e., information system level)and as a result, tend to overlook other significant risk factors that may be more appropriately assessed at Tier 1 or Tier 2 levels (e.g., exposure of a core mission/business function to an adversarial threat based on information system interconnections).

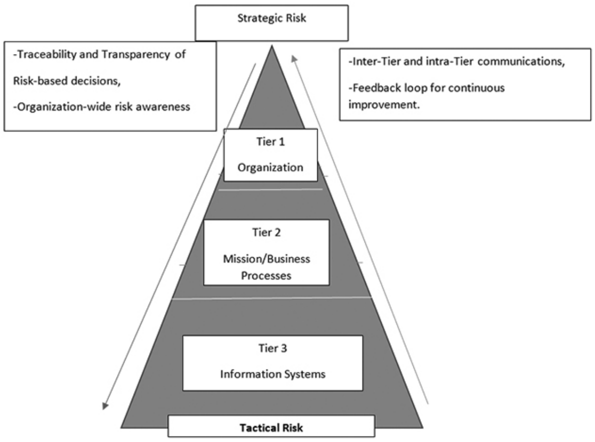
Strategic Risk
-Traceability and Transparency of Risk-based decisions,
-Organization-wide risk awareness
-Inter-Tier and intra-Tier communications,
-Feedback loop for continuous improvement.
Tier 1
Organization
Tier 2
Mission/Business Processes
Tier 3
Information Systems
Tactical Risk

Fig. 4: Risk Management Hierarchy

Risk assessment support risk response decisions at different tiers of the risk management hierarchy. At the Tier 1, risk assessments can affect, for example:

1. Organization-wide-information security programs, procedures, and guidance,

2. The types of appropriate risk responses (i.e., risk acceptance, risk avoidance, mitigation, sharing transfer),

3. Investment decisions for information technologies/systems,

4. Procurement of information, software, communications, etc.,

5. Minimum organization-wide security controls,

6. Conformance to organization/security architectures, and

7. Monitoring strategies and ongoing authorizations of information systems and common controls.

At Tier 2, risk assessments can affect, for example:

1. Organization architecture/security architecture design decisions,

2. The selection of common controls,

3. The selection of suppliers, services, and contractors to support organizational missions/business functions,

4. The development of risk aware mission/business processes, and

5. The implementation of information security policies with respect to organizational information systems and environments in which those systems operate.

Finally, at Tier 3, risk assessments can affect, for example:

1. Design decisions (including the selection, tailoring and supplementation of security controls and the selection of information technology products for organizational information systems),

2. Implementation decisions (including whether specific information technology products or product configurations meet security control requirements), and

3. Operational decisions (including the requisite level of monitoring activity, the frequency of ongoing information system authorizations, and system maintenance decisions).

Risk assessments can also inform other risk management activities across the three tiers that are not-security-related. For example, Tier 1, risk assessment6s can provide useful inputs to:

1. Operational risk determinations (including business continuity for organizational missions and business functions),

2. Organizational risk determinations (including financial risk, compliance risk, regulatory risk, reputations risk, and cumulative acquisition risk across large-scale projects), and

3. Multiple-impact risks (including supply chain risk and risk involving partnerships).

At Tier 2, risk assessment can provide the same useful inputs to operational, organizational and multi-impact risks, specific to mission/business processes.

At Tier 3, risk assessments can inform assessments of cost, schedule, and performance risk associated with information systems, with information security experts coordinating with program managers, information system owners, and authorizing officials. This type of condition is essential with organizations in order to eliminate silos and/or stove-piped activities that produce less than optimal or inefficient information technology and security solutions, thus affecting the ability of organizations to carry out assigned missions/business functions with maximum efficient and cost-effectiveness.

5.1Risk Assessments at the Organizational Tier:

At tier 1, risk assessments support organizational strategies, policies, guidance, and processes for managing risk. Risk assessments conducted at Tier 1, focus on organizational operations, assets, and individuals, comprehensive assessments across mission/business lines. For example, Tier 1 risk assessments may address:

1. The specific type of threats directed at organizations that may be different from other organizations and how those threats affect policy decisions,

2. Systematic weaknesses or deficiencies discovered in multiple organizational information systems capable of being exploited by adversaries,

3. The potential adverse impact on organizations from the less or comprise of organizational information (either internationally or un-internationally),

4. The use of new information and computing technologies such as mobile and cloud and potential effect on the ability of organizations to successfully carry out the mission/business operations while using those technologies.

Organization-wide assessments of risk can be based solely on the assumptions, constraints, risk tolerance, priorities, and tradeoffs established in risk framing step (derived primarily from time activities). However, more realistic and meaningful risk assessments are based on assessments conducted primarily from Tier 2 activities).

The ability to organizations to effectively use Tier 2 risk assessments as inputs to Tier 2 risk assessments is shaped by such considerations:

1. The similarities of organizational missions/business functions and mission/business processes, and

2. The degree of autonomy that organizational entities or subcomponents have with respect to parent organizations.

In decentralized organizations or organizations with varied missions/business functions and/or environments of operation, expert analysis may be needed to normalize the results from Tier 2 risk assessment.

5.2Risk Assessment at the Mission/Business Process Tier:

At Tier 2, risk assessments support the determination of mission/business process protection and resiliency requirements, and allocation of those requirements to the organization architecture as part of mission/business segments (that support mission/business processes). This allocation is accomplished within the organization architecture. Tier 2. Risk assessments also inform and guide decisions on whether, how, and when to use information systems for specific mission/business process, in particular for alternative mission/business processing in the face of compromised information systems. Risk management and associated risk assessment activities at Tier 2 are closely aligned with the development of business community plans. Tier 2 risk assessments focus on mission/business segments, which typically include multiple information systems, with varying degrees of critically and/or sensitivity with regard to core organizational missions/business functions (that is identified in business impact analysis). Risk assessments at Tier 2, can also focus on information security architecture as a critical component of organization architecture to help organizations select common controls inherited by organizational information systems at Tier 3. Risk assessment results produced at Tier 2 are communicated to and shared with organizational entities of Tier 3 to help inform and guide the allocation security controls to information systems and environments in which those systems operate. The Tier 2 risk assessments also provide assessments of security and risk posture of organizational mission/business processes, which inform assessments of organizational risks at Tier 1, risk assessment results at Tier 2 are routinely communicated to organizational entities at Tier 1 and Tier 3.

5.3Risk Assessments at Information Systems Tier:

The Tier 2 context and the system development life cycle determine the purpose and define the scope of risk assessment activities at Tier 3.While initial risk assessments (i.e., risk assessments performed for the 1st time, rather than updating prior risks) can be performed in the initial phase of the system life cycle. In this initial phase, risk assessments evaluate the anticipated vulnerabilities and predisposing conditions affecting confidentiality, integrity and availability of information systems in the context of the planned environments of operations. Such assessments inform risk response, enabling information system owners/program managers, together with mission/business owners to make the final decisions about the security controls necessary based on security categorization and environment of operation. Risk assessments are also conducted at later phases in the risk development life cycle, updating risk assessment results for as built or as deployed information systems typically include descriptions of vulnerabilities in the systems, assessment of risks associated with vulnerability (thereby updating the assessment of vulnerability security), and corrective actions that can between to mitigate the risks. The risk assessment results also include an assessment of the overall risk to the organization and information contained in the information systems by operating the systems as evaluated. Risk assessment results at Tier 3 are communicated to organizational entities at Tier 1 and Tier 2.

Risk assessment activities can be integrated with the stages in Risk Management Framework (RMF). The RMF, in its system development life cycle approach, operate primarily at Tier 3 with some application at Tiers 1 and 2, for example, the selection of common controls. Risk assessment can be tailored to each step or stage in RMF as reflected in the objective and scope of assessments described above. Risk assessments can also help determine the type of security assessments conducted during various phases or stages of the system development life cycle, the frequency of such assessments, the level of rigor applied during assessments, the assessment methods used, and the type/number of objects assessed. The benefit of risk assessments conducted as part of the RMF can be realized from both the initial assessments and from updated assessments.

The following steps or stages of RMF are considered in the following steps or stages:

1. Categorization,

2. Selection,

3. Implementation,

4. Assessment,

5. Authorization, and

6. Monitoring.

5.4Risk Communications and Information Sharing:

The risk assessment process entails ongoing communications and information sharing among stakeholders to ensure that:

1. The inputs to such assessments are as accurately as possible,

2. The intermediate assessment results can be useful, for example, to support risk assessments at other tiers, and

3. The results are meaningful and useful inputs to the risk response step in the risk management process.

6. Risk Assessment Process: Conducting Risk Assessments with Organizations:

The risk assessment process is composed of four steps:

1. Prepare for assessment,

2. Conduct the assessment,

3. Communicate assessment results, and

4. Maintain the assessment.

Each step is divided into a set of tasks. For each task, supplemental guidance provide additional information for organizational conducting risk assessments. The following figure shows the basic steps in risk management process and highlights the specific tasks for conducting the assessment.

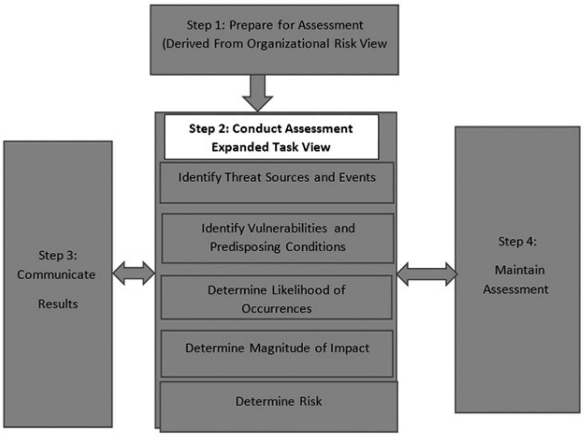
Step 1: Prepare for Assessment
(Derived From Organizational Risk View
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrences
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment

Fig. 5: Risk Assessment Process

6.1Preparing for Risk Assessment:

The objective of this step is to establish a context for risk assessment. This context is established and informed by the results from the risk framing step of risk management process. Risk framing identifies, for example, organizational information regarding policies and requirements for conducting risk assessment specific assessment methodologies to be employed, procedures for selecting risk factors to be considered, scope of assessments, rigor of analyses, degree of formality and requirements that facilitate consistent and repeatable risk determinations across organizations. Therefore, preparing for risk assessment includes the following tasks:

1. Identify the purpose of assessment,

2. Identify the assumptions and constraints associated with assessment,

3. Identify the sources of information to be used as inputs to assessment, and

4. Identify the risk model and analytic approaches (i.e., assessment and analysis approaches) to be employed during the assessment.

6.2 Conducting the Risk Assessment:

The objective of this step is to produce a list of information security risks that can be prioritized by risk level and used to inform risk response decisions. To accomplish this objective, organizations analyze threats and vulnerabilities, impacts and likelihood, and the uncertainty associated with the risk assessment process. This step also includes the gathering of essential information as a part of each task and is conducted in accordance with the assessment context established in the prepare step of the risk assessment process. The execution of risk assessments is to adequately cover the entire threat space in accordance with specific definitions, guidance, and direction established during the prepare step.

Conducting risk assessments includes the following specific tasks:

1. Identify threat sources that are relevant to organizations,

2. Identify threat events that could be produced by those resources,

3. Identify vulnerabilities within organizations that could be exploited by risk sources through specific threat events and predisposing conditions that could affect successful exploitation,

4. Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful,

5. Determine and adverse impacts that organizational operations and assets, individuals, other organizations, and the country resulting from the exploitation of vulnerabilities by threat sources Through specific threat events), and

6. Determine information security risks to a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with risk determinations.

6.3Communicating and Sharing Risk Assessments Information:

The objective of this step is to ensure that the decision makers across the organizations have the appropriate risk related information needed to inform and guide risk decisions. Communicating and sharing information consists of the specific tasks:

1. Communicate the risk assessment results, and

2. Share information developed in the execution of the risk assessment, to support other risk management activities.

6.4Maintaining the Assessment:

The objective of this step is to keep current, the specific knowledge of the risk organizations occur. The results of risk assessments is to inform risk management decisions and guide risk responses. T support the ongoing review of risk management decisions (e.g., acquisition, decisions, authorization decisions for information systems and common controls, connection decisions), organizations maintain risk assessments to incorporate any changes detected through risk monitoring. Risk monitoring provides organizations with the means to, on an ongoing basis:

• Determine the effectiveness of risk responses,

• Identify risk impacting changes to organizational information systems and the environments in which those systems operate, and

• Verify compliance,

Therefore, maintain risk assessments include the following main specific tasks:

1. Monitor risk factors identified in risk assessments on an ongoing basis and understanding subsequent changes to those factors, and

2. Update the components of risk assessments reflecting the monitoring activities carried out by organizations.

6.5Risk Management Framework:

A risk management framework combines all these processes involved in realizing existing as well as newly identified approaches in a manner consistent with public interest, human safety and law, while managing adverse effects or impacts caused by the complexity of existed systems. It involves identifying, assessing and judging risks, assigning ownerships, taking action to mitigate or anticipatethem, and monitoring as well as reviewing progress. The outcome is a holistic analysis that weight the cost of protective measures and establishes a continuous process to manage them.

A risk management framework's complexity needs to match the scale and scope of a service conducted by an individual, organization or a country. Large scale services may employ professional risk analyses or consulting houses.

The key tools in a risk management frameworks identify risks, the financial consequences, and the likelihood of risks occurring. They are used continually input just at the beginning of a service or a project. The tools employed can be a simple spreadsheet up to a formal analysis process, depending on the size and scope of the organizational service.

In contrast, an ad-hoc approach to addressing newly identified risks may overlook the importance of existing risks. It creates new risks such as technology conflicts, obsolescence and inadequate focus on prioritizing solutions according to greatest value.It can also waste time and money, e.g., acquiring expensive security technology to address a low-probability risk. Instead, there must be an organization, or country-wide commitment to applying the risk management framework on a continuous basis. This is the proven method of benefiting from risk management process.

Organizational or national risk assessments help decision makers define and map long-term security strategies, which may identify requirements for adopting new technologies as part of an overall security strategy. These are tailored towards specific compliance requirement, such as fulfilling the requirements under the guidance of a security operational framework standards such as ISO 17799 and ISO 27002 of the ISO's Technical Committee 215 at the year 2005. Documented techniques and methodologies exist for conducting organizational risk assessments, which draw from relevant best practice and industry guidance or requirements.

7. Administrative, Procedural and Technical Controls:

The administrative and technical controls are conforming the policies and controlling the risks.

7.1Administrative Controls:

The administrative controls are non-technical controls that ensure the privacy and security policies that may be enforced during the course of IT acquisition, implementation, and operation to provide assurances that privacy and security policies are being followed. The common criteria for IT security evaluation (ISO/IEC 27001 & 27002: 2005)

Identifies several security administrative controls that should be followed when acquiring and implementing operating systems that are subject to a set of defined policies and objectives as follows:

1. Development: Technical architecture, functional design, structural design, implementation details, security policies, security-relevant features of an IT system.

2. Guidance Documents and Education: Preparation for use and secure operation of an IT system and proper handling of privacy protected organization's services data by employees.

3. Life Cycle Support: Life-cycle definition, configuration management scope and capabilities, development security, security tools and techniques, delivery and security flow remediation for IT system.

4. Security Testing: Coverage, depth, functional tests, and evaluate independence for testing the security functions of an IT system.

5. Vulnerability Assessments: Tasks to be done periodically during IT system development and operation to assess system vulnerabilities (e.g., as part of risk management).

6. Composition: Rationale, evidence, dependencies, testing, and vulnerability analysis for systems that are composed from multiple IT components.

The common criteria also defines discrete levels of assurance for applying these controls. Basically higher levels of assurance will require greater upfront costs and operating costs. Many systems operate at level 3 (methodically tested and checked) which is for circumstances in which developers or users require a moderate level of independently assured security via through investigation of the system and its development, but without substantial reengineering being required. To assurance organization's services and functions privacy and security protections, level 4 (methodically designed, tested and reviewed) may be necessary and further reengineering and retrofitting, at additional cost. Good risk analysis will help determine what level of assurance is required for each circumstance.

7.2Procedural Controls:

In the operation of IT systems, manual or automated procedures must be in place to provide management services and system administrators, including:

- Accountability for following and enforcing of privacy and security policies, assessing specific identities to those who are accessing IT system resources or data. This includes terminating employees who violate privacy and security policies.

- Privacy disclosure log review, notifications, and alerts to discover instances or patterns of privacy breaches and enable prompt and appropriate actions. This includes making disclosure logs available to consumers upon request.

- Security audit log review, notifications, and alerts to discover instances or patterns of attempts or successful security breaches, including inappropriate access by persons who are authorized to access the data, and to enable prompt and appropriate actions.

- Metrics gathering and reporting to monitor trends and patterns in privacy and security incidents and prompt effective administrative actions.

- Processes of making data available, e.g., granting access to authorized persons, importing data from other IT systems, gaining access to data residing on other systems, etc.

- Processes for removing data from shared storage facilities, in particular in response to privacy breaches or consumers' requests. Ongoing public relations programs to communicate with stakeholders regarding ongoing protections, as well as prompt and forthright reporting of privacy violations if they occur.

- Ongoing public relations programs to communicate with stakeholders regarding ongoing protections, as well as prompt and forthright reporting of privacy violations if they occur.

The definition of the required procedural controls should be part of administrative assurance controls.

7.3Technical Controls:

The common criteria for information technology security evaluation (ISO/IEC 15408) identifies also these elements in the way that defines security objectives and evaluates the technology intended to fulfill them as follows:

- Auditing: The collection, storage, analysis and reporting of evidence that the security policies are being enforced and followed, plus evidence of attempts to violate them.

- Identification and Authentication: Means for people (or system entities) to identify themselves prior to system access and for systems to obtain assurances that they and in fact, who the claim to be. It includes rules for strength of passwords and other authentication data.

- Data Protection: Means to grant or withhold permission for access, ensure intra-system confidentiality, protect integrity, ensure authenticity, enable secure import and disclosures of data. This includes technologies as e-mail filters and anti-virus protection.

- Management: The set of functions to manage all security functions, generally restricted to authorized administrators. This includes user provisioning for identifies, passwords, authorizations.

- Cryptographic Support: The generation, provision, communication, and use of cryptographic technologies to protect data confidentiality and integrity. This especially includes using encryption over the public Internet and protecting wireless networks from snooping by un-authorized people.

- Nonrepudiation: Proof that a claimed providers of data, who did, in fact,send it and it has not been altered. Similarly, proof that an intended recipient of data who did, in fact, receive it.

- Privacy: Technical means to provide anonymity, pseudonimity, unlinkability, and unobservability of system users and data. An information system privacy rule may define data that must be removed for anonymity when data is reused, e.g., aggregated for research functional activity.

- Protection of Security System Itself: Ensuring that the security system is not a weak point in an otherwise secure system.

- Resource Utilization: Ensuring that systems are available and that there are controls to prevent accidental or deliberate unavailability of system services due to overutilization.

- System Access: Prevention for multiple access-points for individual users (signed-on at multiple workstations), session and workstation locking when security violations are detected, notification of security policies when user-sign-on, and masking passwords when entered.

- Trusted Paths: The means to establish and maintain secure network connections among systems components and with other trusted systems.

Therefore, any information system certification criteria cover only a subset of the above factors.

7.4Handling Redidual Risk Controls:

Various non-technical measures to mitigate risks that cannot be effectively or economically handled by other controls, e.g., insurance. Therefore, after all mitigations defined previouslyhave been established, there remains a set of risks that cannot be practically or economically addressed. These redidual risks can be mitigated by other means, including the following:

- Additional/Incremental Controls: Monitoring the IT product market and trade journals for new and less expensive security technology, additional training, best practices, etc.

- Delegation: Enrolling business partners in any organization system or vendors to assume additional risks via trust agreement or business associate agreement amendments.

- Insurance: Transferring the financial consequences of risks to an insurance organization, especially pooling risks with other organizations.

- More Acceptance: Some risks are so unlikely, even if they may have catastrophic consequences, that it is prudent merely to accept them.

8. Conclusion:

Businesses and nations today are driven by a global economy that generates an overwhelming volume, variety and velocity of data. This explosive data growth has led to an equal explosive growth of ways to use this data for operational and strategic gain. Although the emerging mix of information, service and delivery technologies across mobile, social and cloud-based environments open innovative new business opportunities, it also changes user behavior, and with it, nations and organizations' security risks, security needs to adopt a world that is evolving faster than before.

Once IT organizations have an overall picture of the security risks through threats and vulnerabilities they face on a daily and a broader understanding of how these risks might affect the business, they need to act against these risks. This is done by risk assessments to:

- Protect critical infrastructure and sensitive business information proactively,

- Automate many of the more costly, time-consuming aspects of nation's and organization's security,

- Identify the genuine risks (threats, vulnerabilities, etc.) in a magnitude of malware, viruses, and exploits, either acting on them automatically or giving IT detailed guidance about where and how to respond, and

- Reduce the costs and capabilities of meeting compliance targets that vary across jurisdictions and geographic boundaries.

When technology moves faster every day, security needs also to keep pace. An IT organization that better understands the risks associated with innovation is more certain that its threat or risk assessment is as timely as it is accurate, and that its defenses against data breaches are as rapid as they are through with security for a faster world. Therefore, IT organizations can stop saying "no" to new-technologies and start saying a careful, considered, and confident "yes" to new ways of helping the business take the lead.

Hence, leverage risk assessment and threat modeling to ensure that efforts are spent in the right directions and places. Given the complexity of most organizations, and sheer number of overall vulnerabilities, it is important to be able to prioritize risks in order to determine what gets remediated and when. Key to any successful security management is the knowledge that cannot fix everything overnight and the ability to focus attention on the things that present the most danger and harm to the organization and the nation as well.

Therefore, mitigate the risks by applying appropriate security controls (administrative, procedural and technical controls) to each data category is very essential. Security costs money, and that means that ultimate security is about risk management assessments, i.e., ensuring sufficient controls are applied to each data category to reduce the risk of a breach to an acceptable level.Security can almost always be improved, but the question is always whether it can be done in a cost-effectiveness manner, i.e., you do not need to apply platinum-level security to public data.

Although, all of the forthcomings four aspects and steps are very important as protective and safeguards controls to any organization or nation, the fourth step is the one that is the hardest to carry out, because it involves implementing the entire security infrastructure (software and hardware) that will actually keep the business secure. These main steps are as follows:

1. A firewall and other perimeter security systems to separate any organization network from the Internet,

2. Malware scanners to prevent malicious software from getting on to the network hidden in e-mail, instant messaging or Web traffic.

3. An Intrusion Preventing System (IPS), to detect malicious, suspicious or simply unusual activity on the network and to take steps to prevent such activity leading to a security breach, and

4. The use of authentication and encryption systems to prevent unauthorized access to networks, computers and data stored on them and on the organization's information systems.

For smaller businesses, a lot of this functionality can probably be achieved with Unified Threat Management (UTM) appliance while provides basic firewall, antimalware and IPS services.An alternative is to engage a Managed Security Service Provider (MSSP) to configure and manage the security devices and provide log management as well.

Larger businesses, have more decisions to make. They should look for security partner that can supply the basic infrastructure expert deployment advice and professional services, as well as additional monitoring features and services such as the followings:

1. A security information and event management platform to monitor and report on relevant security events and logs.

2. A business centric risk management platform to identify risks to the business that originate in the IT infrastructure.

3. Protecting for the mobile and cloud-based environment resources>

References:

- ISF (2007). Information Security forum standard of good practice for information security. [http://www.securityforum.org/services/publictools/publicstandardofgoodpractice/]
- ISO/IEC 15408 (2006). Common criteria for information technology security evaluation, version 3.1. Geneva, ISO
- ISO 15408-1 (2009). ISO/IEC 15048-1: 2009. Information technology - security techniques - evaluation criteria for IT security - Introduction and General model. Geneva: ISO
- ISO/IEC 17799: 2005 (ISO 27002).Security policy coverage defining roles and responsibilities. Geneva: ISO
- ISO 27001 (2005). ISO/IEC 2700: 2005. Information technology - security techniques - information security management systems - requirements. Geneva: ISO
- ISO 27002 (2005). ISO/IEC 27002:2005. Information technology - security techniques - code for information security management. Geneva: ISO
- ISO/IEC 27005: 2011; Information technology- security techniques - information security risk management. Geneva, ISO
- ISO/IEC 27005: 2011. A framework for implementing a risk management approach in managing information security management (ISMS) risks. Geneva: ISO
- ISO/IEC 31000: 2009; Risk management: Principles and guidance. Geneva, ISO
- ISO/IEC 30101: 2009; Risk management: Risk assessment techniques. Geneva, ISO
- ISO/IEC 29100: 2011 Security Techniques - Privacy Framework.