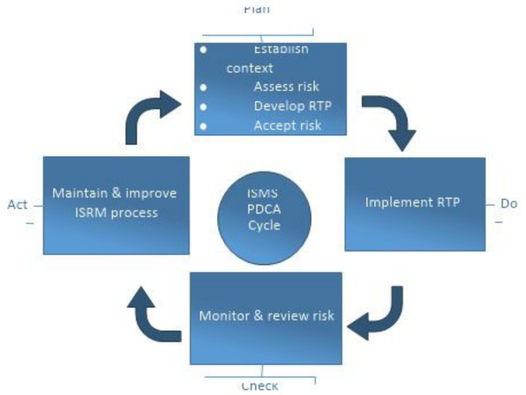
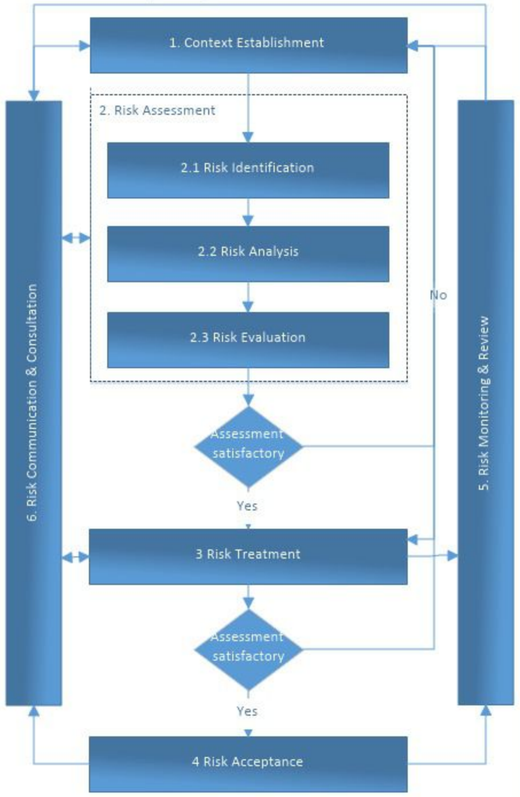
Risk management process within ISMS PDCA cycle



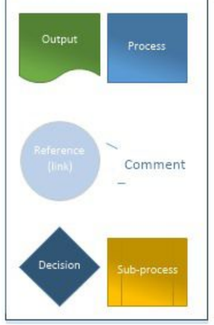
Information Security Management Process



Description

Study of the organization
purpose, business, missions, values, strategies, structure
Asset classification
Primary assets: business process & activities, information
Supporting assets: hardware, software, network, personnel, site, structure
Constraints
Organization -> political, cultural, personnel, strategical, territorial, economical, financial, structural, functional, timing, methodical etc.
Scope -> pre-existing processes, technical, financial, environmental constraints, time, methodical, organizational etc.
Risk modification -> time, financial, technical, operational, cultural, ethical, environmental, legal , ease of use, personnel, existing controls etc.
References
http://www.iso27001security.com/html/27005.html
ISO/IEC 27005:2011, Information technology -- Security techniques -- Information security risk management

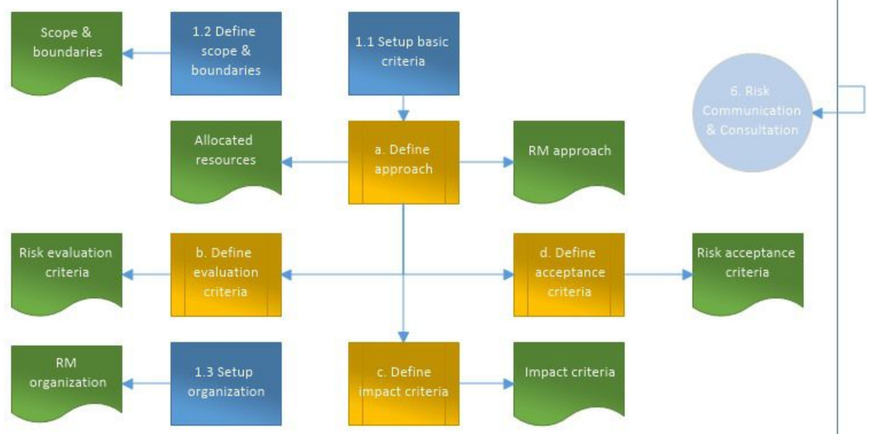
Legend



Acronyms

- BCP: Business Continuity Plan
- C.I.A: Confidentiality, Integrity & Availability
- IEC: International Electrotechnical Commission
- InfoSec: Information Security
- IRP: Incident Response Plan
- ISMS: Information Security Management System
- ISO: International Organization for Standardization
- ISRM: Information Security Risk Management
- PDCA: Plan-Do-Check-Act
- RM: Risk Management
- RPM: Risk Management Plan
- RTP: Risk Treatment Plan

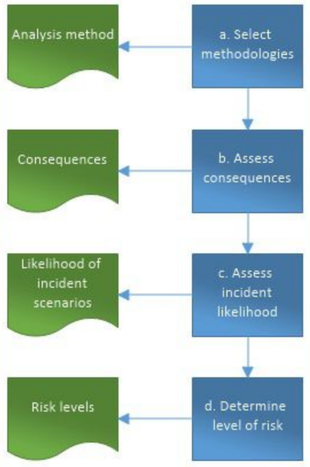
1. Context Establishment



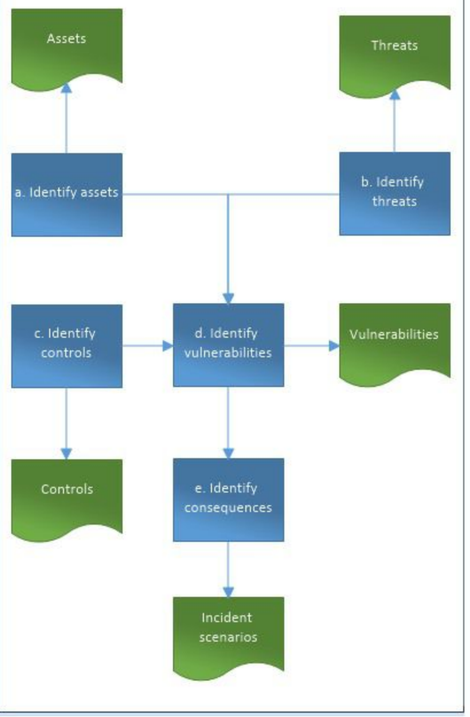
2. Risk Assessment

2.3 Risk Evaluation

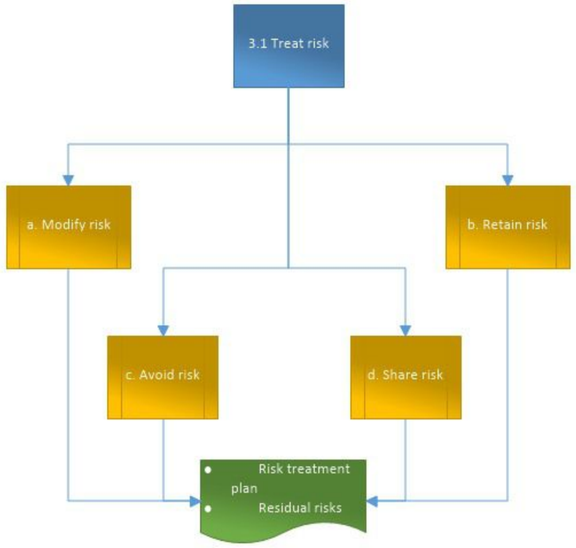
2.2 Risk Analysis



2.1 Risk Identification



3. Risk Treatment

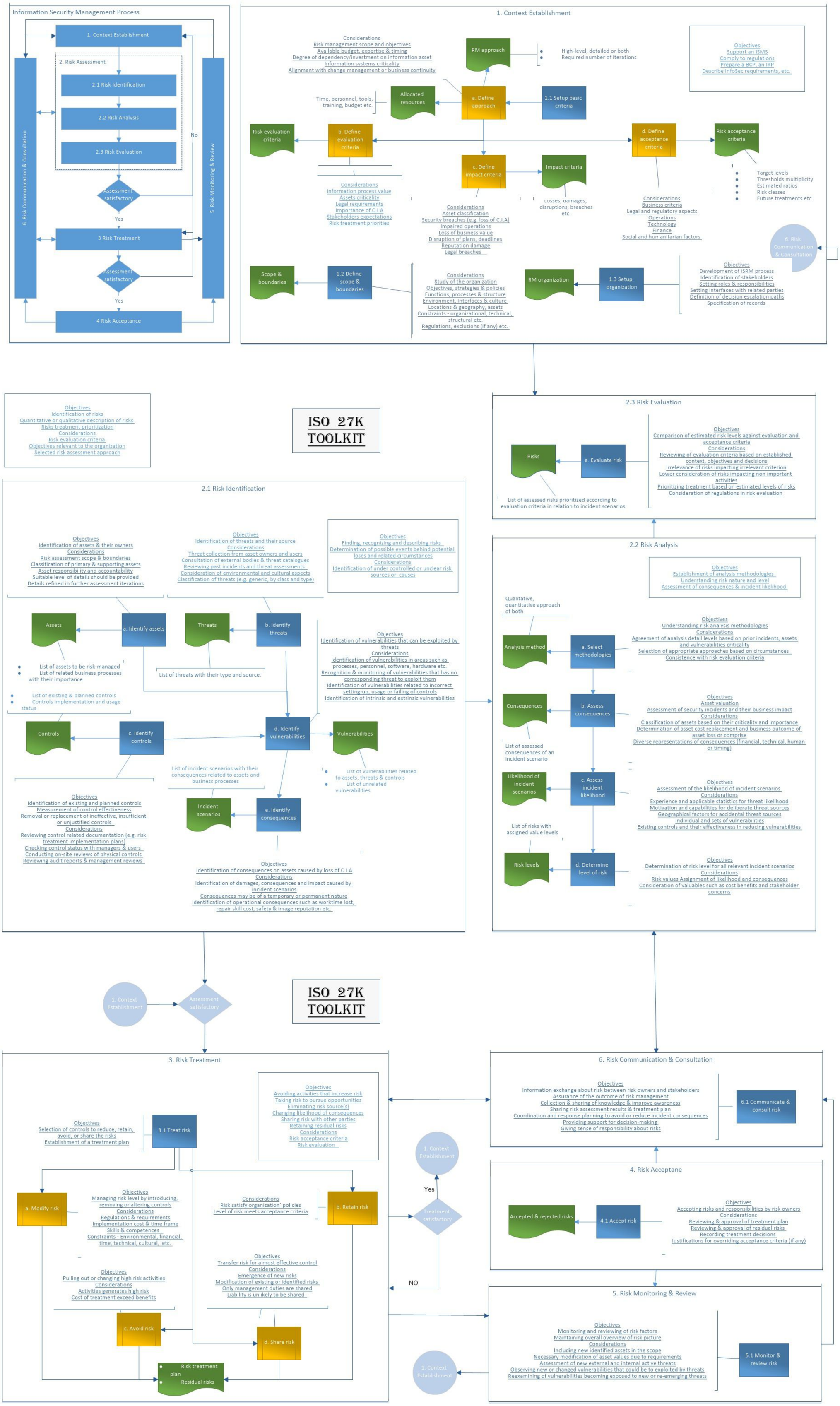


5. Risk Monitoring & Review

4. Risk Acceptane

6. Risk Communication & Consultation

ISO 27K TOOLKIT


Information Security Management Process
1. Context Establishment
2. Risk Assessment
2.1 Risk Identification
2.2 Risk Analysis
2.3 Risk Evaluation
Assessment satisfactory
Yes
No
3 Risk Treatment
Assessment satisfactory
Yes
4 Risk Acceptance
6. Risk Communication & Consultation
5. Risk Monitoring & Review
1. Context Establishment
Considerations
Risk management scope and objectives
Available budget, expertise & timing
Degree of dependency/investment on information asset
Information systems criticality
Alignment with change management or business continuity
RM approach
High-level, detailed or both
Required number of iterations
Objectives
Support an ISMS
Comply to regulations
Prepare a BCP, an IRP
Describe InfoSec requirements, etc.
Time, personnel, tools, training, budget etc.
Allocated resources
a. Define approach
1.1 Setup basic criteria
Risk evaluation criteria
b. Define evaluation criteria
d. Define acceptance criteria
Risk acceptance criteria
c. Define impact criteria
Impact criteria
Considerations
Information process value
Assets criticality
Legal requirements
Importance of C.I.A
Stakeholders expectations
Risk treatment priorities
Considerations
Asset classification
Security breaches (e.g. loss of C.I.A)
Impaired operations
Loss of business value
Disruption of plans, deadlines
Reputation damage
Legal breaches
Losses, damages, disruptions, breaches etc.
Considerations
Business criteria
Legal and regulatory aspects
Operations
Technology
Finance
Social and humanitarian factors
Target levels
Thresholds multiplicity
Estimated ratios
Risk classes
Future treatments etc.
6. Risk Communication & Consultation
Scope & boundaries
1.2 Define scope & boundaries
Considerations
Study of the organization
Objectives, strategies & policies
Functions, processes & structure
Environment, interfaces & culture
Locations & geography, assets
Constraints - organizational, technical, structural etc.
Regulations, exclusions (if any) etc.
RM organization
1.3 Setup organization
Objectives
Development of ISRM process
Identification of stakeholders
Setting roles & responsibilities
Setting interfaces with related parties
Definition of decision escalation paths
Specification of records
ISO 27K TOOLKIT
Objectives
Identification of risks
Quantitative or qualitative description of risks
Risks treatment prioritization
Considerations
Risk evaluation criteria
Objectives relevant to the organization
Selected risk assessment approach
2.3 Risk Evaluation
Risks
a. Evaluate risk
List of assessed risks prioritized according to evaluation criteria in relation to incident scenarios
Objectives
Comparison of estimated risk levels against evaluation and acceptance criteria
Considerations
Reviewing of evaluation criteria based on established context, objectives and decisions
Irrelevance of risks impacting irrelevant criterion
Lower consideration of risks impacting non important activities
Prioritizing treatment based on estimated levels of risks
Consideration of regulations in risk evaluation
2.1 Risk Identification
Objectives
Identification of assets & their owners
Considerations
Risk assessment scope & boundaries
Classification of primary & supporting assets
Asset responsibility and accountability
Suitable level of details should be provided
Details refined in further assessment iterations
Objectives
Identification of threats and their source
Considerations
Threat collection from asset owners and users
Consultation of external bodies & threat catalogues
Reviewing past incidents and threat assessments
Consideration of environmental and cultural aspects
Classification of threats (e.g. generic, by class and type)
Objectives
Finding, recognizing and describing risks
Determination of possible events behind potential loses and related circumstances
Considerations
Identification of under controlled or unclear risk sources or causes
Assets
a. Identify assets
Threats
b. Identify threats
List of assets to be risk-managed
List of related business processes with their importance
List of threats with their type and source.
Objectives
Identification of vulnerabilities that can be exploited by threats
Considerations
Identification of vulnerabilities in areas such as processes, personnel, software, hardware etc.
Recognition & monitoring of vulnerabilities that has no corresponding threat to exploit them
Identification of vulnerabilities related to incorrect setting-up, usage or failing of controls
Identification of intrinsic and extrinsic vulnerabilities
List of existing & planned controls
Controls implementation and usage status
Controls
c. Identify controls
d. Identify vulnerabilities
Vulnerabilities
List of incident scenarios with their consequences related to assets and business processes
List of vulnerabilities related to assets, threats & controls
List of unrelated vulnerabilities
Incident scenarios
e. Identify consequences
Objectives
Identification of existing and planned controls
Measurement of control effectiveness
Removal or replacement of ineffective, insufficient or unjustified controls
Considerations
Reviewing control related documentation (e.g. risk treatment implementation plans)
Checking control status with managers & users
Conducting on-site reviews of physical controls
Reviewing audit reports & management reviews
Objectives
Identification of consequences on assets caused by loss of C.I.A
Considerations
Identification of damages, consequences and impact caused by incident scenarios
Consequences may be of a temporary or permanent nature
Identification of operational consequences such as worktime lost, repair skill cost, safety & image reputation etc.
2.2 Risk Analysis
Objectives
Establishment of analysis methodologies
Understanding risk nature and level
Assessment of consequences & incident likelihood
Qualitative, quantitative approach of both
Analysis method
a. Select methodologies
Objectives
Understanding risk analysis methodologies
Considerations
Agreement of analysis detail levels based on prior incidents, assets and vulnerabilities criticality
Selection of appropriate approaches based on circumstances
Consistence with risk evaluation criteria
Consequences
b. Assess consequences
List of assessed consequences of an incident scenario
Objectives
Asset valuation
Assessment of security incidents and their business impact
Considerations
Classification of assets based on their criticality and importance
Determination of asset cost replacement and business outcome of asset loss or comprise
Diverse representations of consequences (financial, technical, human or timing)
Likelihood of incident scenarios
c. Assess incident likelihood
Objectives
Assessment of the likelihood of incident scenarios
Considerations
Experience and applicable statistics for threat likelihood
Motivation and capabilities for deliberate threat sources
Geographical factors for accidental threat sources
Individual and sets of vulnerabilities
Existing controls and their effectiveness in reducing vulnerabilities
List of risks with assigned value levels
Risk levels
d. Determine level of risk
Objectives
Determination of risk level for all relevant incident scenarios
Considerations
Risk values Assignment of likelihood and consequences
Consideration of valuables such as cost benefits and stakeholder concerns
1. Context Establishment
Assessment satisfactory
ISO 27K TOOLKIT
3. Risk Treatment
Objectives
Avoiding activities that increase risk
Taking risk to pursue opportunities
Eliminating risk source(s)
Changing likelihood of consequences
Sharing risk with other parties
Retaining residual risks
Considerations
Risk acceptance criteria
Risk evaluation
Objectives
Selection of controls to reduce, retain, avoid, or share the risks
Establishment of a treatment plan
3.1 Treat risk
a. Modify risk
Objectives
Managing risk level by introducing, removing or altering controls
Considerations
Regulations & requirements
Implementation cost & time frame
Skills & competences
Constraints - Environmental, financial, time, technical, cultural, etc.
Considerations
Risk satisfy organization' policies
Level of risk meets acceptance criteria
b. Retain risk
Objectives
Pulling out or changing high risk activities
Considerations
Activities generates high risk
Cost of treatment exceed benefits
Objectives
Transfer risk for a most effective control
Considerations
Emergence of new risks
Modification of existing or identified risks
Only management duties are shared
Liability is unlikely to be shared
c. Avoid risk
d. Share risk
Risk treatment plan
Residual risks
1. Context Establishment
Yes
Treatment satisfactory
NO
1. Context Establishment
6. Risk Communication & Consultation
Objectives
Information exchange about risk between risk owners and stakeholders
Assurance of the outcome of risk management
Collection & sharing of knowledge & improve awareness
Sharing risk assessment results & treatment plan
Coordination and response planning to avoid or reduce incident consequences
Providing support for decision-making
Giving sense of responsibility about risks
6.1 Communicate & consult risk
4. Risk Acceptane
Accepted & rejected risks
4.1 Accept risk
Objectives
Accepting risks and responsibilities by risk owners
Considerations
Reviewing & approval of treatment plan
Reviewing & approval of residual risks
Recording treatment decisions
Justifications for overriding acceptance criteria (if any)
5. Risk Monitoring & Review
Objectives
Monitoring and reviewing of risk factors
Maintaining overall overview of risk picture
Considerations
Including new identified assets in the scope
Necessary modification of asset values due to requirements
Assessment of new external and internal active threats
Observing new or changed vulnerabilities that could be to exploited by threats
Reexamining of vulnerabilities becoming exposed to new or re-emerging threats
5.1 Monitor & review risk