NEXUSGUARD
CONSULTING

如何在您的組織環境中合規應用ISO/IEC27001
Practical Implementation of ISO/IEC 27001 in Your Environment

Security Standards Council
APPROVED SCANNING VENDOR

Security Standards Council
PAYMENT APPLICATION QUALIFIED SECURITY ASSESSOR

Security Standards Council
QUALIFIED SECURITY ASSESSOR

觸動社會責任企業大獎
Touching CSR Award
(Reference to ISO 26000 clause 6)
2013

bsi.
ISO/IEC 27001
Information Security Management

About Me

Experience d Specialities

- Ronald is an Information Security Professional who has 18 years of experience in this business. His responsible field included Information Security Management, Compliance Audit, Computer Forensics, Anti - Hacking, Training and Classical Cryptographer. Ronald has a out standing track record in Information Technology field has helped enhance the reputations of such firms and organisations as International Banking, Finances, Government, Educa1on, Manufacturing and Law's Enforcement in Great China Area.
- **Professional Filed:** *Computer Forensic investigator / Professional Lecturer / Information Security and Hacking Expert / Credit Card Payment Security Professional / Inventor / Classical Cryptographers*

Ronald Pong

- **Professional certificates:**
  - Payment Card Application Security Assessor (PA QSA)
  - PCI Qualified Security Assessor (PCI QSA)
  - PCI Approved Scanning Vendors (ASV)
  - ISO/IEC 27001 ISMS Lead Auditor Certificate
  - ISO/IEC 20000 ITSM Auditor
- **Membership:**
  - British Computer Society (BCS)
  - Chinese Association for Crypto logic Research (CACR) (中国密码学会)
  - Information System Security Association (ISSA)
  - International Association for Crypto logic Research (IACR)
  - Hong Kong Public Key Infrastructure Forum (HKPKI)
  - Institute of Electrical and Electronics Engineers (IEEE)
  - International Register of Certificated Auditors (IRCA)
  - Hong Kong Information and System Security Professional Association (HKISSP)
  - Payment Card Industry Professional (PCIP)

Practical Implementation of ISO/IEC 27001 in Your Environment

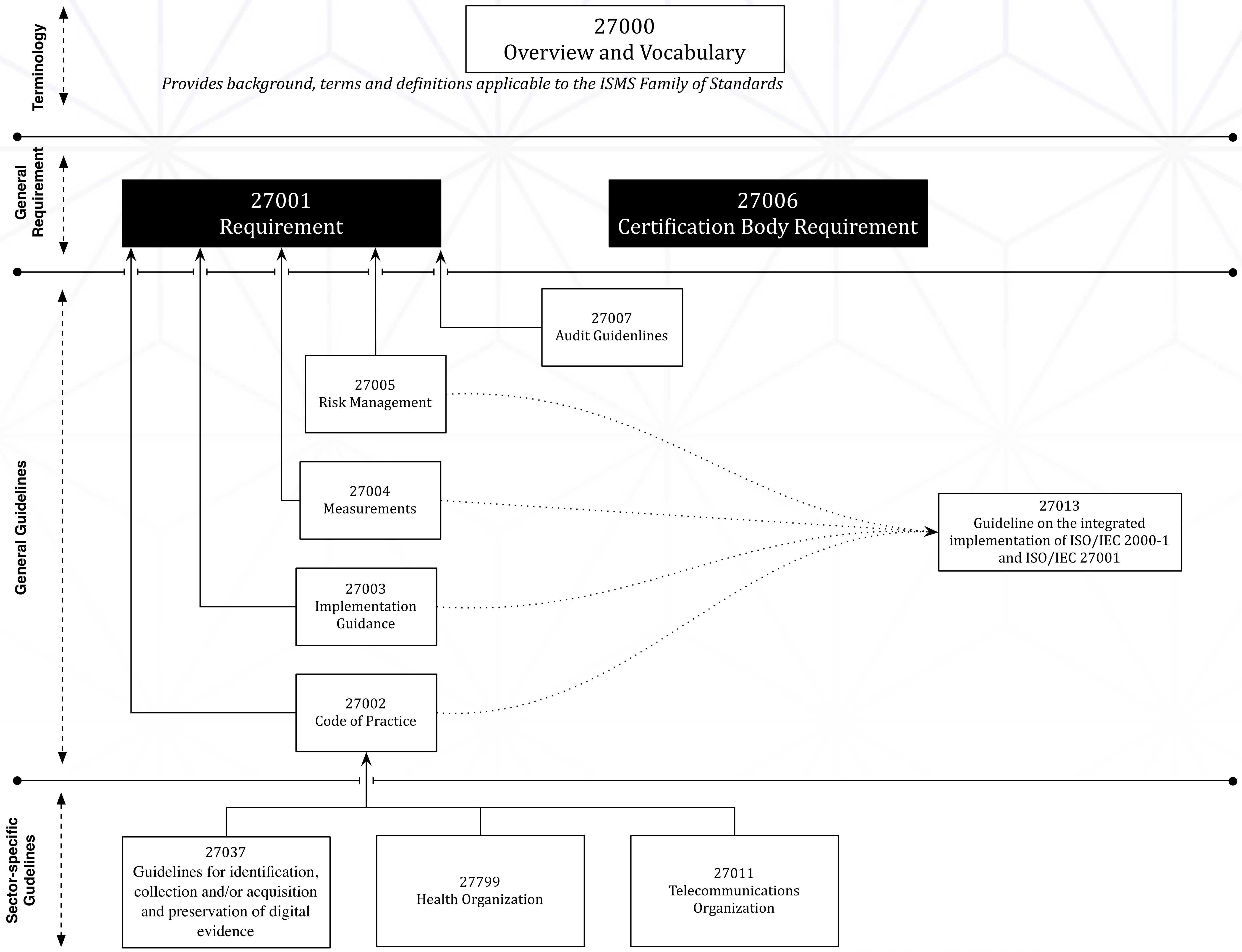
Agenda

- ISO/IEC 27000 : 2014 or ISO/IEC 27001:2013, what is the difference?
- The difference between various documents in ISO/IEC 27000 : 2014 series, How do we use them ?
  - All you need is ISO 27001, 27002, 27003, 27004 and 27005
- Do you know what is the difference between Vulnerability and Threat ?
- Process is everything, what is your major business process? Let us learn more from ISO/IEC 27005 : 2011
- Develop the Threat Model based on the ISO/IEC 27004 Requirement
- Using ISO/IEC 27005:2011 as Impact Analysis and Risk Assessment Requirement
- Q&A

ISO/IEC 27000 : 2014 or ISO/IEC 27001:2013, what is the difference?

ISO/IEC 27000 : 2014

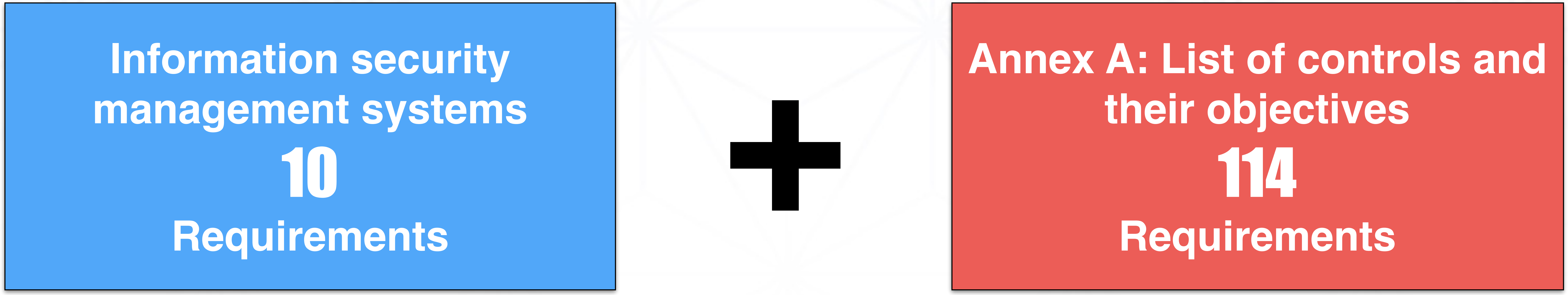
- ISO/IEC 27000 is part of a growing family of ISO/IEC Information Security Management Systems (ISMS) standards, the 'ISO/IEC 27000 series'/ ISO/IEC 27000 is an international standard entitled: Information technology - Security techniques - Information security management systems - Overview and vocabulary.
- The standard was developed by sub-committee 27 (SC27) of the first Joint Technical Committee (JTC1) of the International Organization for Standardization and the International Electrotechnical Commission.
- ISO/IEC 27000 provides:
  - An overview of and intriduction to the entire ISO/IEC 27000 family of Information Security Management Systems (ISMS) standards.
  - A glossary or vocabulary of fundamental terms and definitions used throughout the ISO?IEC 27000 family.


Terminology
27000
Overview and Vocabulary
Provides background, terms and definitions applicable to the ISMS Family of Standards
General Requirement
27001
Requirement
27006
Certification Body Requirement
General Guidelines
27007
Audit Guidenlines
27005
Risk Management
27004
Measurements
27003
Implementation Guidance
27002
Code of Practice
27013
Guideline on the integrated implementation of ISO/IEC 2000-1 and ISO/IEC 27001
Sector-specific Guidelines
27037
Guidelines for identification, collection and/or acquisition and preservation of digital evidence
27799
Health Organization
27011
Telecommunications Organization

ISO/IEC 27000 : 2014 or ISO/IEC 27001:2013, what is the difference?

ISO/IEC 27001 : 2013

- ISO 27001:2013 is an information security standard that was published on the 25th September 2013. It supersedes ISO/IEC 27001:2005, and is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee, ISO/IEC JTC 1/SC 27. It is a specification for an information security management system (ISMS). Organisations which meet the standard may gain an official certification issued by an independent and accredited certification body on successful completion of a formal audit process.



Information security management systems
10
Requirements

+

Annex A: List of controls and their objectives
114
Requirements

Do you know that what is the difference between Vulnerability and Threat ?

Information Security 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. - CISA 2006 Review Manual

- Risk - is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset).

Vulnerability

- A vulnerability is a weakness that could be used to endanger or cause harm to an informational asset.

Threat

- A threat is anything (man made or act of nature) that has the potential to cause harm.

- Management

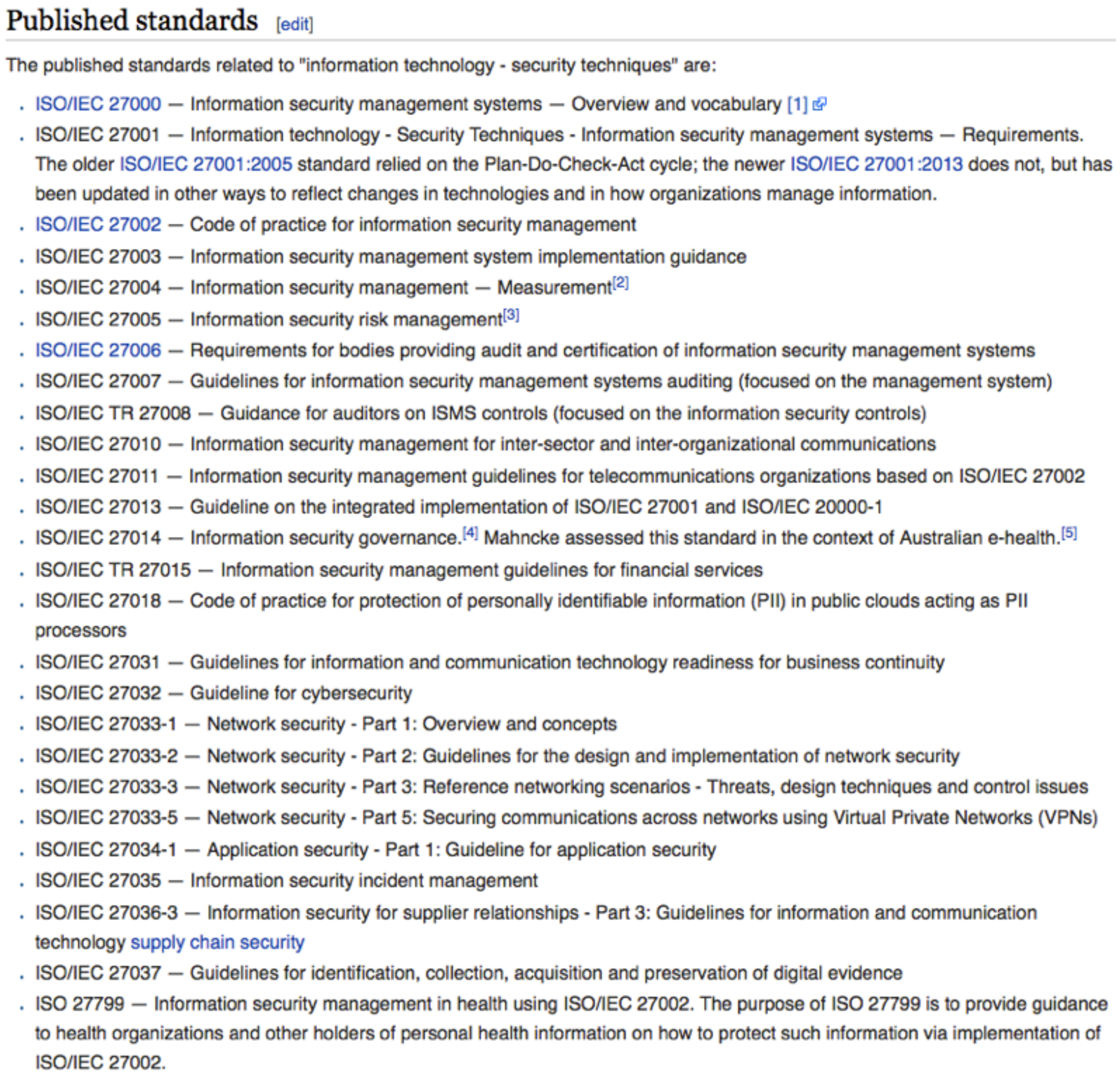
  The term "management" characterizes the process of and/or the personnel leading and directing all or part of an organization (often a business) through the deployment and manipulation of resources (human, capital, natural, intellectual or intangible).

  - **Process**
    - The process of risk management is an ongoing iterative processr It must be repeated indeinitely.

  Choice of control
    - Control is used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

All you need is ISO 27001, 27002, 27003, 27004 and 27005

ISO/IEC 27000 : 2014



Published standards [edit]

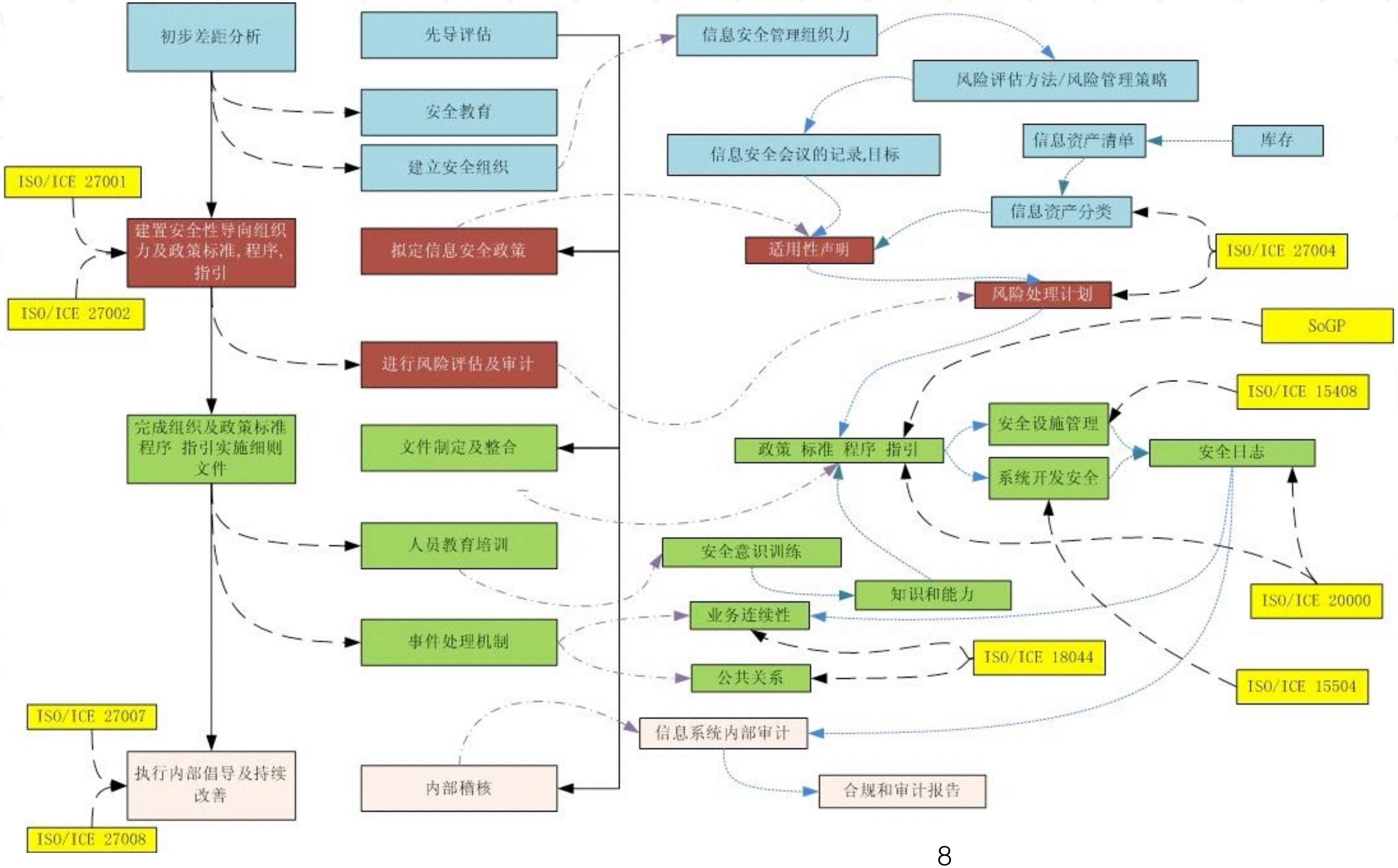
The published standards related to "information technology - security techniques" are:

- ISO/IEC 27000 — Information security management systems — Overview and vocabulary [1]
- ISO/IEC 27001 — Information technology - Security Techniques - Information security management systems — Requirements. The older ISO/IEC 27001:2005 standard relied on the Plan-Do-Check-Act cycle; the newer ISO/IEC 27001:2013 does not, but has been updated in other ways to reflect changes in technologies and in how organizations manage information.
- ISO/IEC 27002 — Code of practice for information security management
- ISO/IEC 27003 — Information security management system implementation guidance
- ISO/IEC 27004 — Information security management — Measurement[2]
- ISO/IEC 27005 — Information security risk management[3]
- ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007 — Guidelines for information security management systems auditing (focused on the management system)
- ISO/IEC TR 27008 — Guidance for auditors on ISMS controls (focused on the information security controls)
- ISO/IEC 27010 — Information security management for inter-sector and inter-organizational communications
- ISO/IEC 27011 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013 — Guideline on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 27014 — Information security governance.[4] Mahncke assessed this standard in the context of Australian e-health.[5]
- ISO/IEC TR 27015 — Information security management guidelines for financial services
- ISO/IEC 27018 — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27031 — Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 27032 — Guideline for cybersecurity
- ISO/IEC 27033-1 — Network security - Part 1: Overview and concepts
- ISO/IEC 27033-2 — Network security - Part 2: Guidelines for the design and implementation of network security
- ISO/IEC 27033-3 — Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues
- ISO/IEC 27033-5 — Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
- ISO/IEC 27034-1 — Application security - Part 1: Guideline for application security
- ISO/IEC 27035 — Information security incident management
- ISO/IEC 27036-3 — Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security
- ISO/IEC 27037 — Guidelines for identification, collection, acquisition and preservation of digital evidence
- ISO 27799 — Information security management in health using ISO/IEC 27002. The purpose of ISO 27799 is to provide guidance to health organizations and other holders of personal health information on how to protect such information via implementation of ISO/IEC 27002.

🟥 **MUST** 🟦 **MAJOR** 🟪 **REFERENCE** 🟧 **SUPPORTIVE**

- ISO/IEC 27001 — Information technology - Security Techniques - Information security management systems
- ISO/IEC 27002 — Code of practice for information security management
- ISO/IEC27003 — Information security management system implementation guidance
- ISO/IEC 27004 — Information security management — Measurement
- ISO/IEC 27005 — Information security risk management
- ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007 — Guidelines for information security management systems auditing
- ISO/IEC 27035 — Information security incident management
- ISO/IEC 27037 — Guidelines for identification, collection, acquisition and preservation of digital evidence

All you need is ISO 27001, 27002, 27003, 27004 and 27005



初步差距分析

先导评估

安全教育

建立安全组织

信息安全管理组织力

风险评估方法/风险管理策略

信息安全会议的记录,目标

信息资产清单

库存

信息资产分类

ISO/ICE 27001

建置安全性导向组织力及政策标准,程序,指引

ISO/ICE 27002

拟定信息安全政策

适用性声明

ISO/ICE 27004

风险处理计划

SoGP

进行风险评估及审计

ISO/ICE 15408

完成组织及政策标准程序 指引实施细则文件

文件制定及整合

政策 标准 程序 指引

安全设施管理

系统开发安全

安全日志

人员教育培训

安全意识训练

知识和能力

ISO/ICE 20000

业务连续性

事件处理机制

ISO/ICE 18044

公共关系

ISO/ICE 15504

ISO/ICE 27007

信息系统内部审计

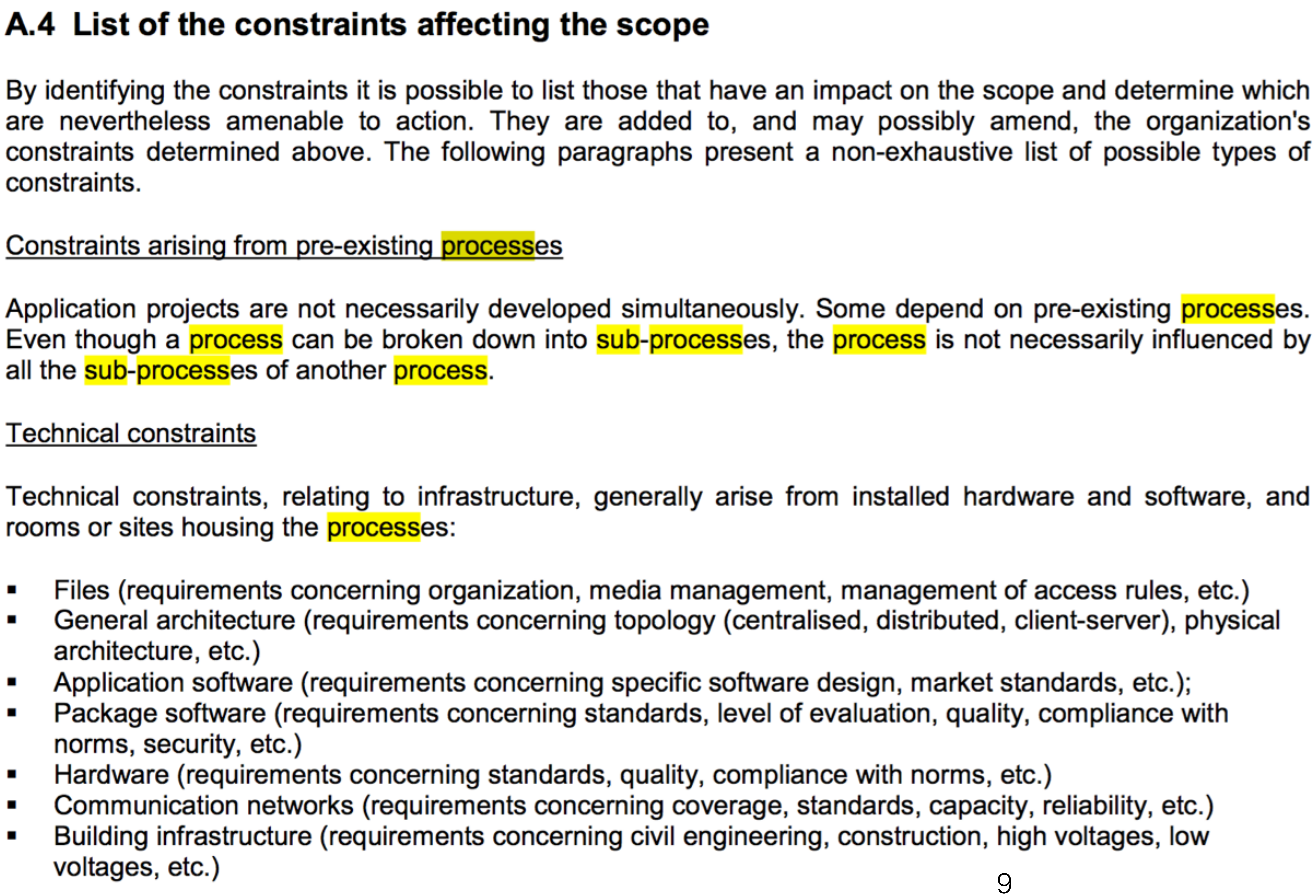
执行内部倡导及持续改善

合规和审计报告

ISO/ICE 27008

内部稽核

Process is everything, what is your major business process? Let us learn more from ISO/IEC 27005 : 2011



A.4 List of the constraints affecting the scope

By identifying the constraints it is possible to list those that have an impact on the scope and determine which are nevertheless amenable to action. They are added to, and may possibly amend, the organization's constraints determined above. The following paragraphs present a non-exhaustive list of possible types of constraints.

Constraints arising from pre-existing processes

Application projects are not necessarily developed simultaneously. Some depend on pre-existing processes. Even though a process can be broken down into sub-processes, the process is not necessarily influenced by all the sub-processes of another process.

Technical constraints

Technical constraints, relating to infrastructure, generally arise from installed hardware and software, and rooms or sites housing the processes:

- Files (requirements concerning organization, media management, management of access rules, etc.)
- General architecture (requirements concerning topology (centralised, distributed, client-server), physical architecture, etc.)
- Application software (requirements concerning specific software design, market standards, etc.);
- Package software (requirements concerning standards, level of evaluation, quality, compliance with norms, security, etc.)
- Hardware (requirements concerning standards, quality, compliance with norms, etc.)
- Communication networks (requirements concerning coverage, standards, capacity, reliability, etc.)
- Building infrastructure (requirements concerning civil engineering, construction, high voltages, low voltages, etc.)

Scoping is everything
ISO 27005 page 28

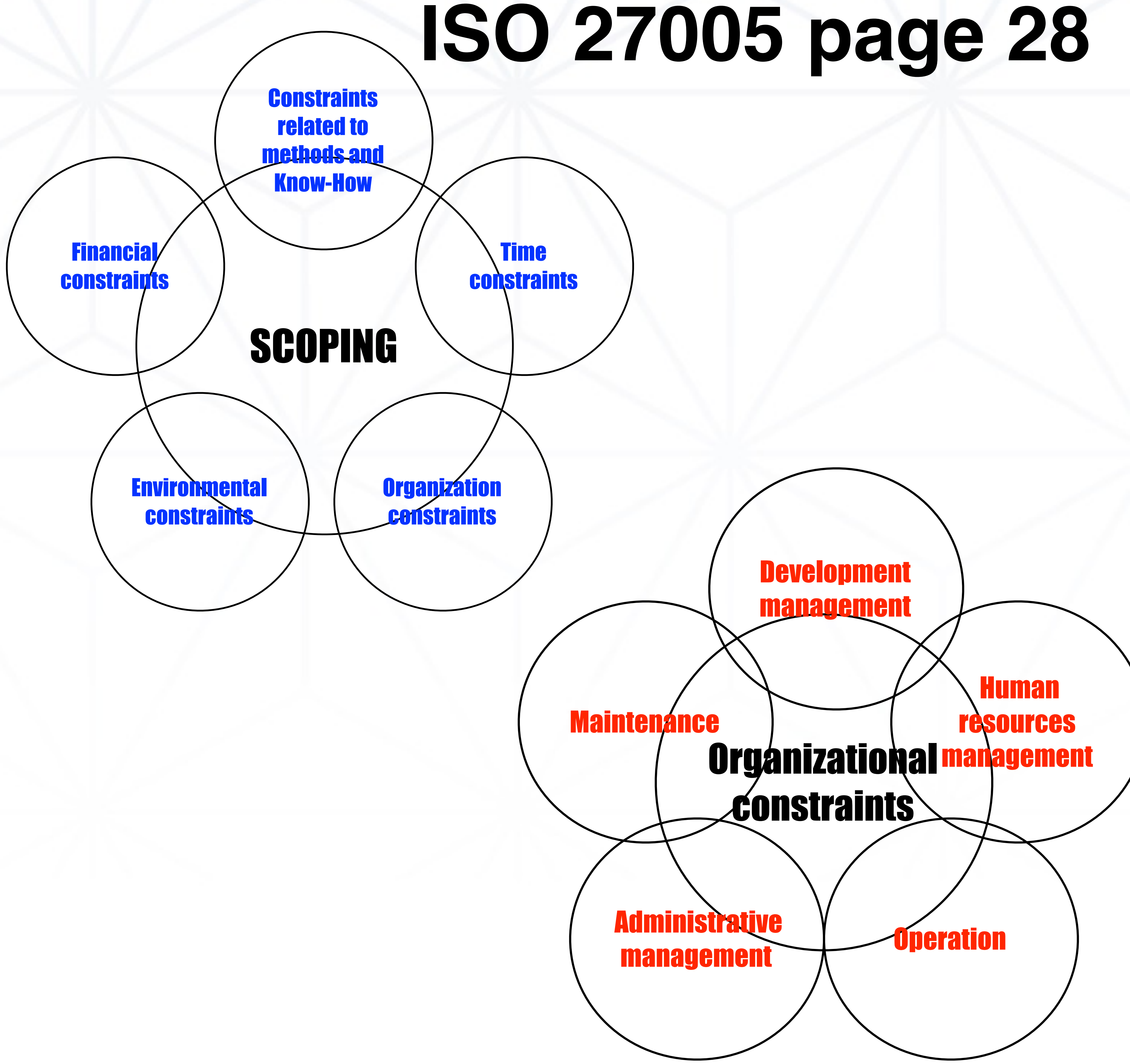
OBJECTIVE

Process is everything, what is your major business process? Let us learn more from ISO/IEC 27005 : 2011

The scope and boundaries

- The organization should define the scope and boundaries of information security risk management.
- The scope of the information security risk management process needs to be defined to ensure that all relevant assets are taken into account in the risk assessment. In addition, the boundaries need to be identified [see also ISO/IEC 27001 Clause 4.2.1 a)] to address those risks that might arise through these boundaries.
- Information about the organization should be collected to determine the environment it operates in and its relevance to the information security risk management process.
- When defining the scope and boundaries, the organization should consider the following information:
  - *The organization's strategic business objectives, strategies and policies*
  - *Business processes*
  - *The organization’s functions and structure*
  - *Legal, regulatory and contractual requirements applicable to the organization The organization's information security policy*
  - *The organization’s overall approach to risk management*
  - *Information assets*
  - *Locations of the organization and their geographical characteristics Constraints affecting the organization*
  - *Expectation of stakeholders*
  - *Socio-cultural environment*
  - *Interfaces (i.e. information exchange with the environment)*
- Additionally, the organization should provide justification for any exclusion from the scope.
  - **Examples of the risk management scope may be an IT application, IT infrastructure, a business process, or a defined part of an organization.**

Scoping is everything ISO 27005 page 28



SCOPING

Constraints related to methods and Know-How

Financial constraints

Time constraints

Environmental constraints

Organization constraints

Organizational constraints

Development management

Maintenance

Human resources management

Administrative management

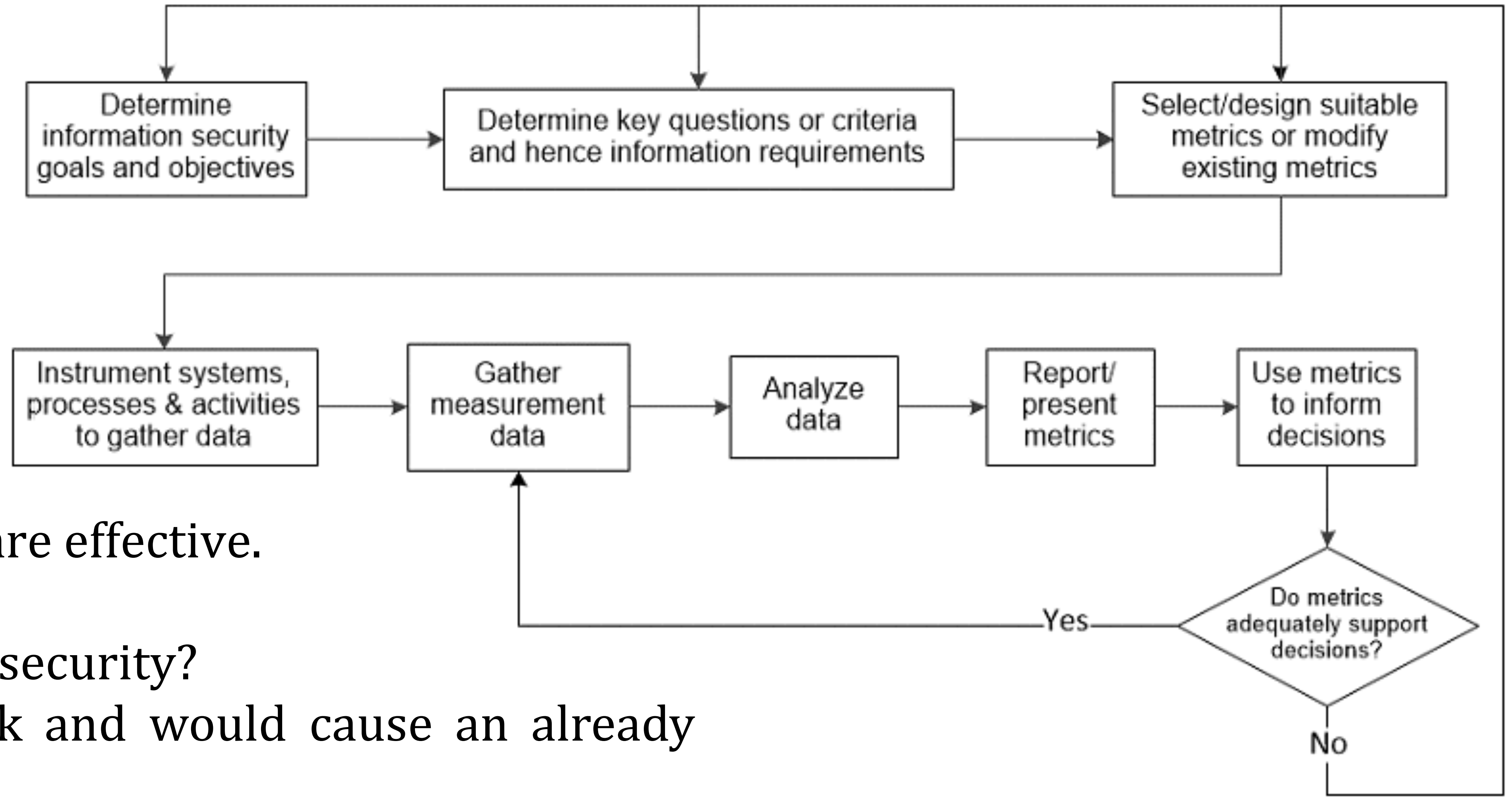
Operation

NEXUSGUARD CONSULTING

Develop the Threat Model based on the ISO/IEC 27004 requirement

MEASUREMENT OF INFORMATION SECURITY MANAGEMENT SYSTEM
How to Measuring the Effectiveness of Security in ISO 27001
Objective of Measurement

- To show ongoing improvement;
- To show compliance (with Standards, contracts, SLAs, OLAs, etc);
- To justify any future expenditure (new security software, training, people, etc);
- ISO 27001 requires it. Other Management Systems also require it – ISO 9001, ISO 20000;
- To identify where implemented controls are not effective in meeting their objectives;
- To provide confidence to senior management and stakeholders that implemented controls are effective.


Determine information security goals and objectives
Determine key questions or criteria and hence information requirements
Select/design suitable metrics or modify existing metrics
Instrument systems, processes & activities to gather data
Gather measurement data
Analyze data
Report/ present metrics
Use metrics to inform decisions
Do metrics adequately support decisions?
Yes
No

So, which of the 114 potentially applicable controls (within ISO 27001) can be used to measure security?
Well, arguably, all of them. In practice, though, this would invariably be too onerous a task and would cause an already overworked IT Department to crumble under the weight of bureaucracy.
Before we attempt to answer this question, then, we should always understand the requirement for such clarity.

- Why are you being asked to provide such information?
- What is the driver?
- Where does the requirement come from?

Other drivers may exist, too. It could be that the company has just realized that you can get more from ISO 27001, or perhaps it's operational risk management such as BASEL II, SOX, Turn bull (UK Corporate Governance) or simply Regulatory requirements and Legislation that's driving your business. Either way, you're not alone. Many organizations (but not all) misunderstand the fundamental concepts behind BS 7799 and ISO 27001 and have treated it as a marketing exercise, as opposed to trying to achieve real business benefit and ROI. ISO 27001 provides much more clarity and goes further into what should be measured for its effectiveness. As such, the much anticipated **ISO 27004** (guidelines on how to measure effectiveness) in 2007 should finally put an end to this 'grey' area and will hopefully shed much needed light onto the types of controls to be measured and what results we should expect (e.g. Industry Baseline).

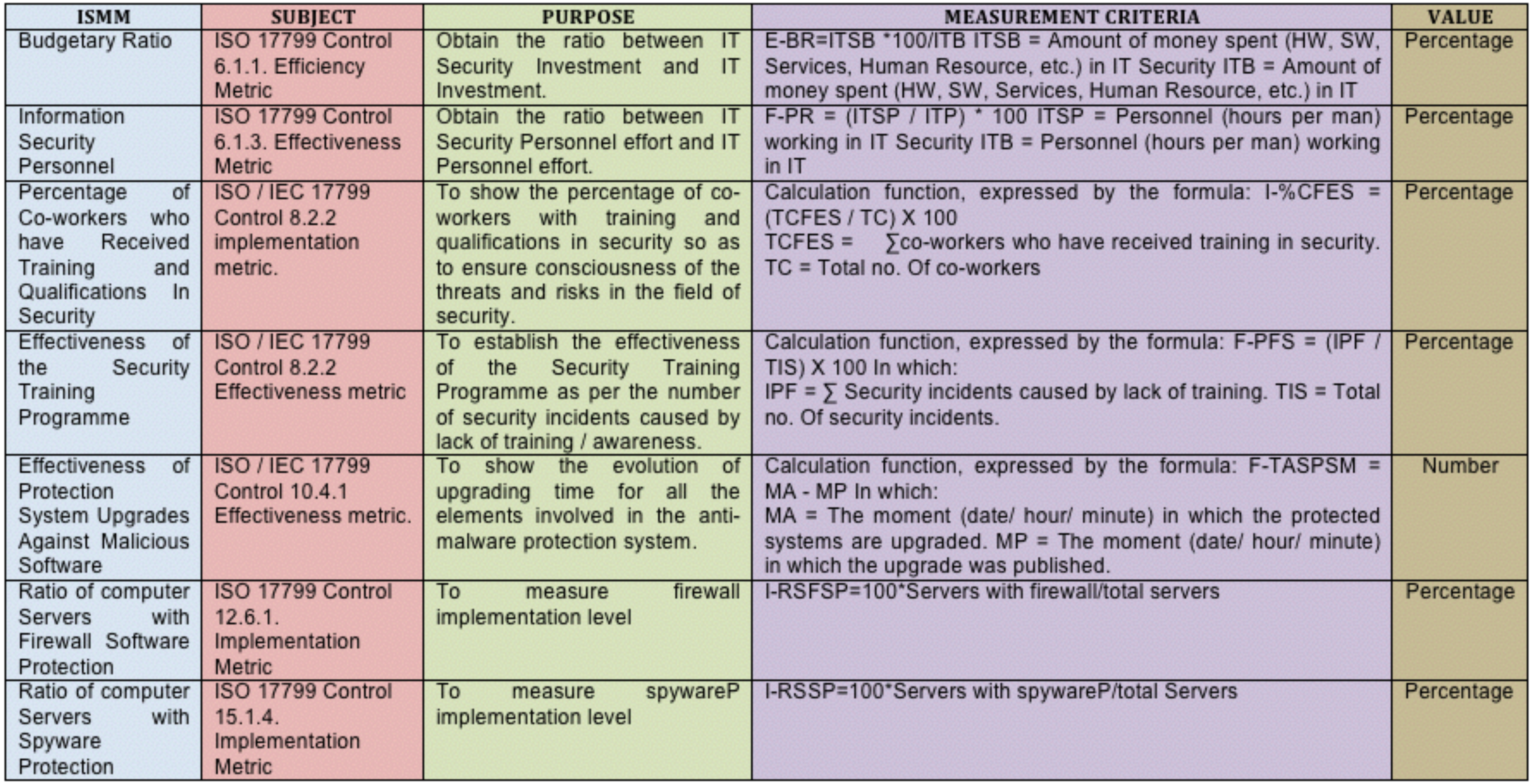
天下萬
物皆有
數

NEXUSGUARD CONSULTING

Develop the Threat Model based on the ISO/IEC 27004 requirement

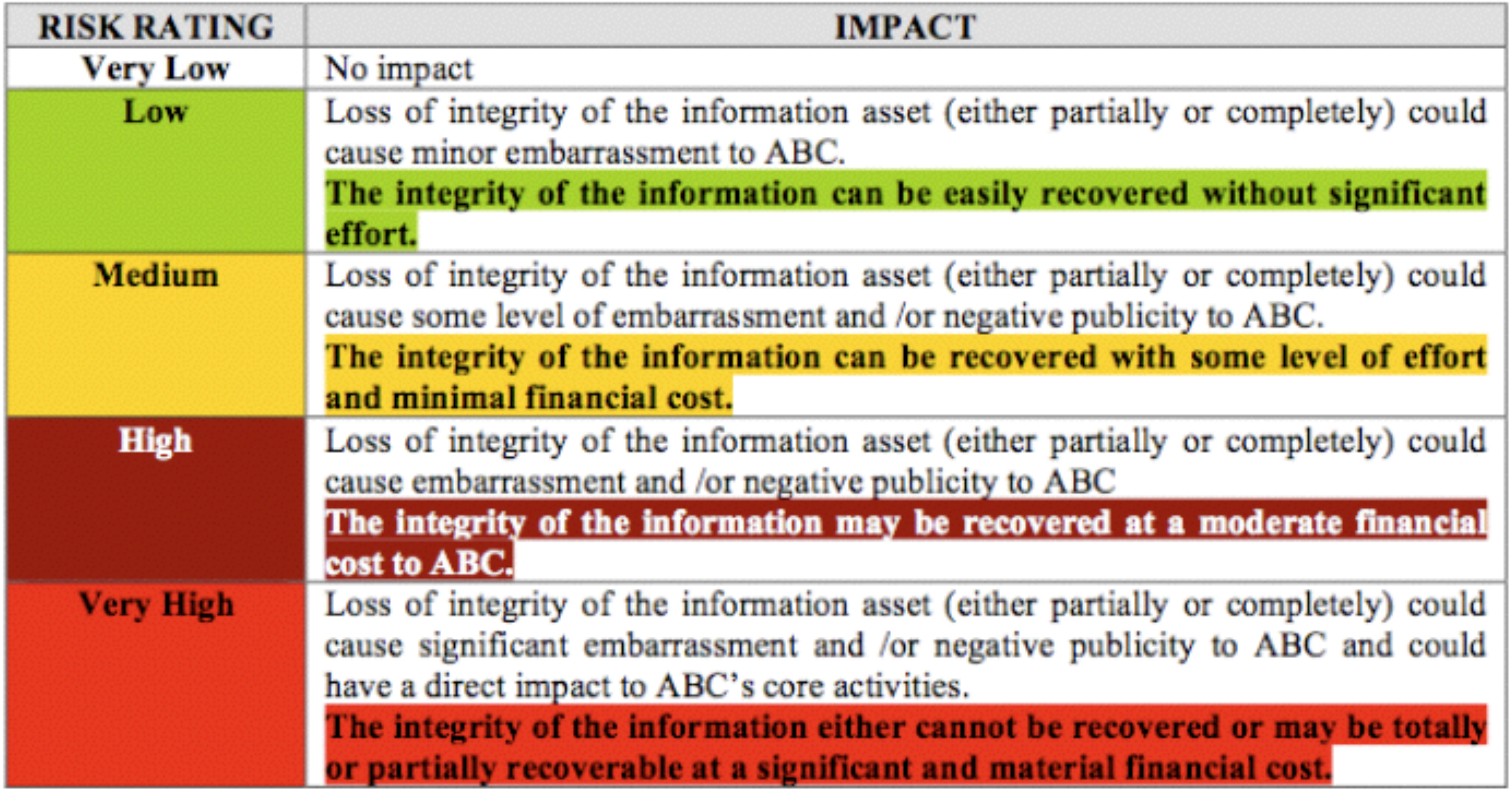
MEASUREMENT OF INFORMATION SECURITY MANAGEMENT SYSTEM

ISO 27004 Information technology - Security techniques - Information security



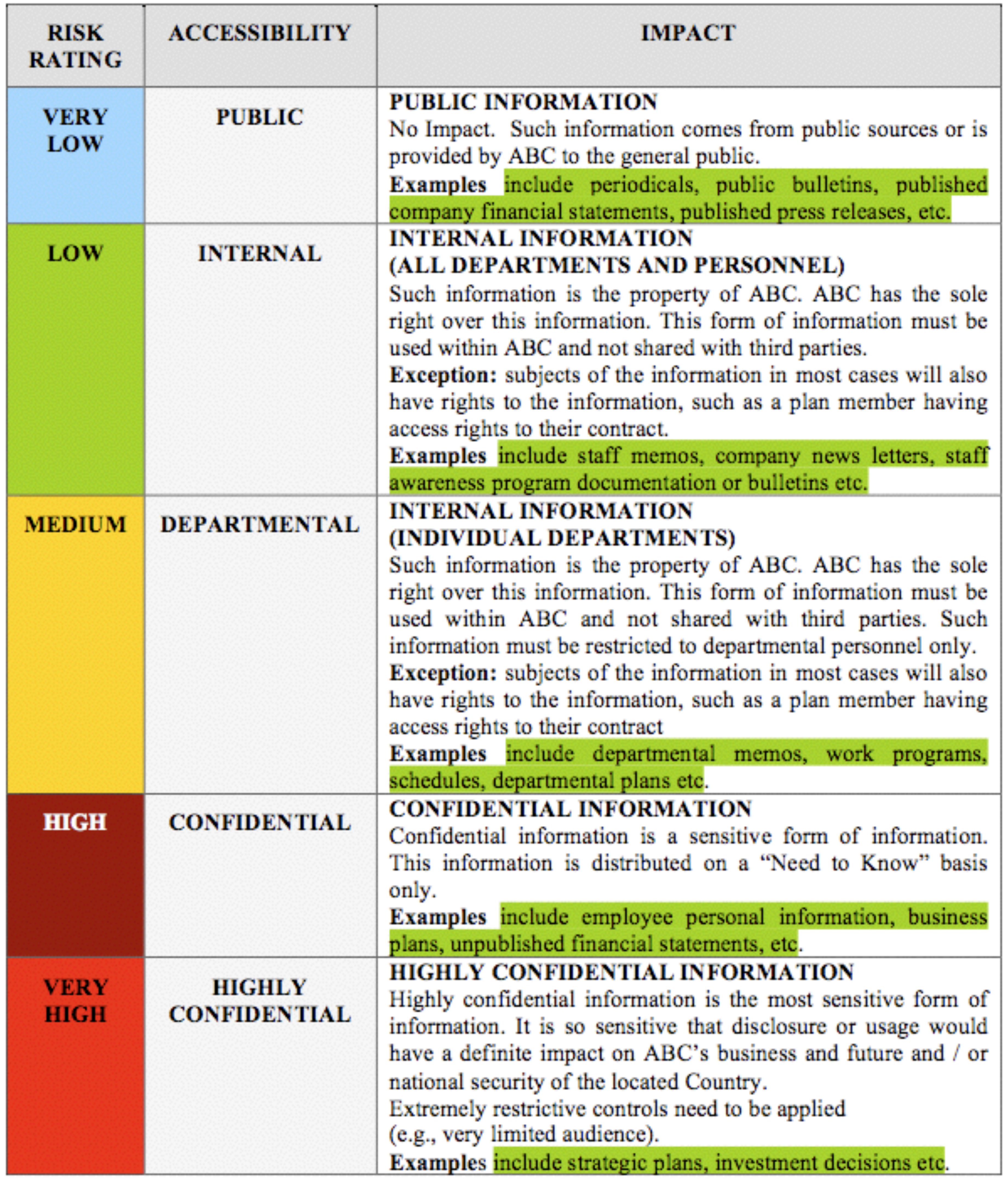
ISMM	SUBJECT	PURPOSE	MEASUREMENT CRITERIA	VALUE
Budgetary Ratio	ISO 17799 Control 6.1.1. Efficiency Metric	Obtain the ratio between IT Security Investment and IT Investment.	E-BR=ITSB *100/ITB ITSB = Amount of money spent (HW, SW, Services, Human Resource, etc.) in IT Security ITB = Amount of money spent (HW, SW, Services, Human Resource, etc.) in IT	Percentage
Information Security Personnel	ISO 17799 Control 6.1.3. Effectiveness Metric	Obtain the ratio between IT Security Personnel effort and IT Personnel effort.	F-PR = (ITSP / ITP) * 100 ITSP = Personnel (hours per man) working in IT Security ITB = Personnel (hours per man) working in IT	Percentage
Percentage of Co-workers who have Received Training and Qualifications In Security	ISO / IEC 17799 Control 8.2.2 implementation metric.	To show the percentage of co-workers with training and qualifications in security so as to ensure consciousness of the threats and risks in the field of security.	Calculation function, expressed by the formula: I-%CFES = (TCFES / TC) X 100 TCFES = ∑co-workers who have received training in security. TC = Total no. Of co-workers	Percentage
Effectiveness of the Security Training Programme	ISO / IEC 17799 Control 8.2.2 Effectiveness metric	To establish the effectiveness of the Security Training Programme as per the number of security incidents caused by lack of training / awareness.	Calculation function, expressed by the formula: F-PFS = (IPF / TIS) X 100 In which: IPF = ∑ Security incidents caused by lack of training. TIS = Total no. Of security incidents.	Percentage
Effectiveness of Protection System Upgrades Against Malicious Software	ISO / IEC 17799 Control 10.4.1 Effectiveness metric.	To show the evolution of upgrading time for all the elements involved in the anti-malware protection system.	Calculation function, expressed by the formula: F-TASPSM = MA - MP In which: MA = The moment (date/ hour/ minute) in which the protected systems are upgraded. MP = The moment (date/ hour/ minute) in which the upgrade was published.	Number
Ratio of computer Servers with Firewall Software Protection	ISO 17799 Control 12.6.1. Implementation Metric	To measure firewall implementation level	I-RSFSP=100*Servers with firewall/total servers	Percentage
Ratio of computer Servers with Spyware Protection	ISO 17799 Control 15.1.4. Implementation Metric	To measure spywareP implementation level	I-RSSP=100*Servers with spywareP/total Servers	Percentage

Develop the Threat Model based on the ISO/IEC 27004 requirement

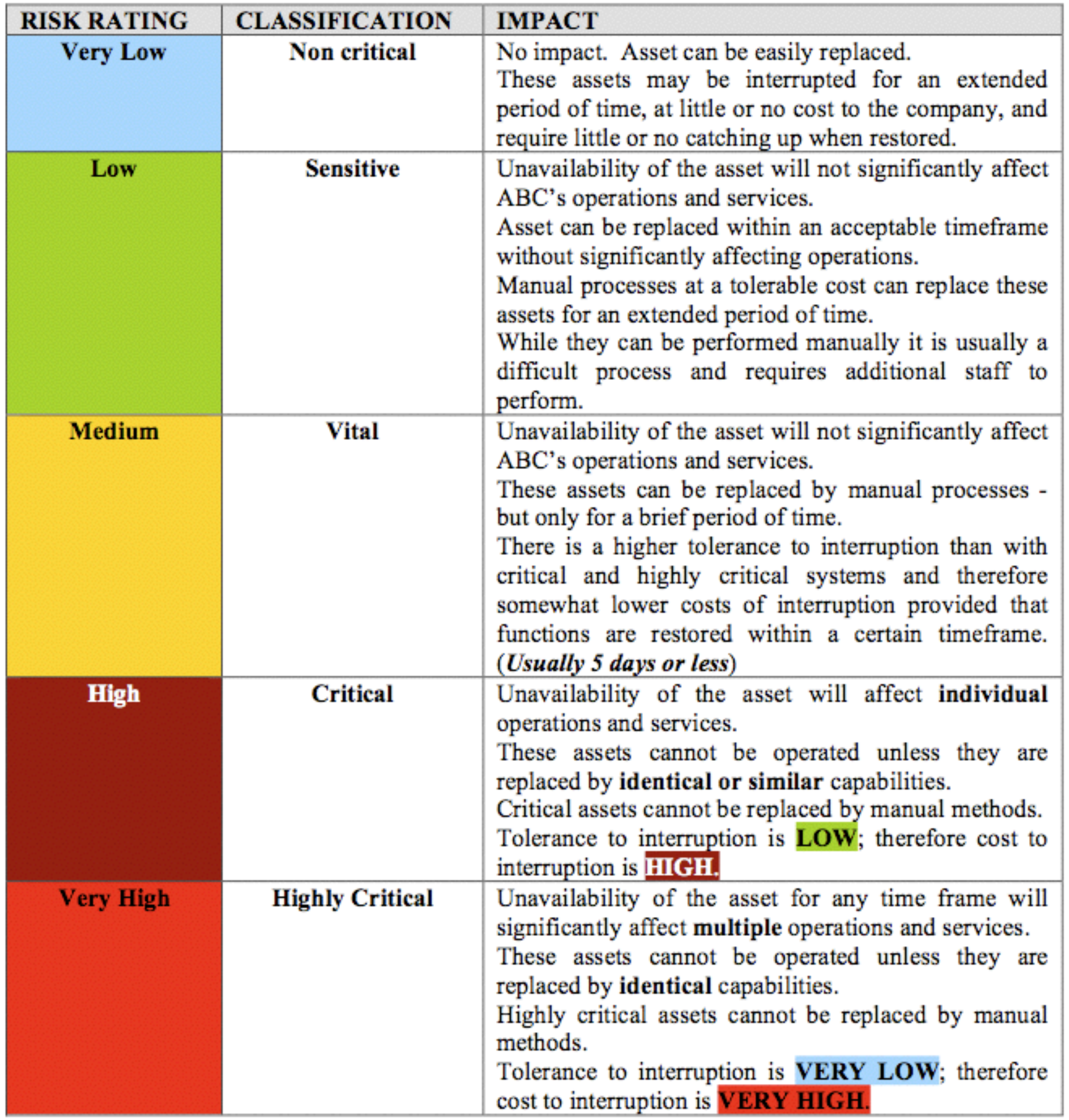


RISK RATING	IMPACT
Very Low	No impact
Low	Loss of integrity of the information asset (either partially or completely) could cause minor embarrassment to ABC. **The integrity of the information can be easily recovered without significant effort.**
Medium	Loss of integrity of the information asset (either partially or completely) could cause some level of embarrassment and /or negative publicity to ABC. **The integrity of the information can be recovered with some level of effort and minimal financial cost.**
High	Loss of integrity of the information asset (either partially or completely) could cause embarrassment and /or negative publicity to ABC **The integrity of the information may be recovered at a moderate financial cost to ABC.**
Very High	Loss of integrity of the information asset (either partially or completely) could cause significant embarrassment and /or negative publicity to ABC and could have a direct impact to ABC's core activities. **The integrity of the information either cannot be recovered or may be totally or partially recoverable at a significant and material financial cost.**

Develop the Threat Model based on the ISO/IEC 27004 requirement



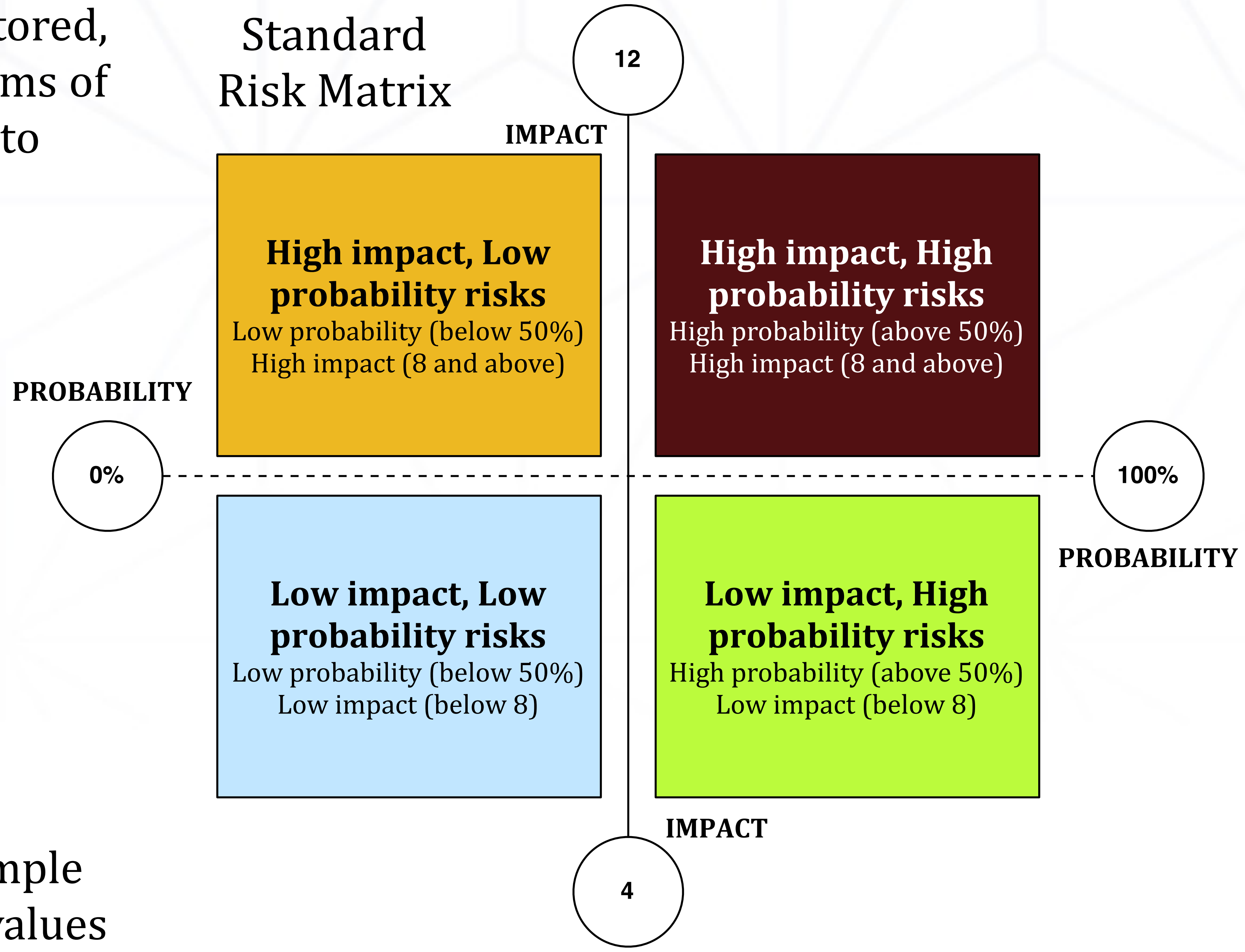
RISK RATING	ACCESSIBILITY	IMPACT
VERY LOW	PUBLIC	**PUBLIC INFORMATION** No Impact. Such information comes from public sources or is provided by ABC to the general public. **Examples** include periodicals, public bulletins, published company financial statements, published press releases, etc.
LOW	INTERNAL	**INTERNAL INFORMATION (ALL DEPARTMENTS AND PERSONNEL)** Such information is the property of ABC. ABC has the sole right over this information. This form of information must be used within ABC and not shared with third parties. **Exception:** subjects of the information in most cases will also have rights to the information, such as a plan member having access rights to their contract. **Examples** include staff memos, company news letters, staff awareness program documentation or bulletins etc.
MEDIUM	DEPARTMENTAL	**INTERNAL INFORMATION (INDIVIDUAL DEPARTMENTS)** Such information is the property of ABC. ABC has the sole right over this information. This form of information must be used within ABC and not shared with third parties. Such information must be restricted to departmental personnel only. **Exception:** subjects of the information in most cases will also have rights to the information, such as a plan member having access rights to their contract **Examples** include departmental memos, work programs, schedules, departmental plans etc.
HIGH	CONFIDENTIAL	**CONFIDENTIAL INFORMATION** Confidential information is a sensitive form of information. This information is distributed on a "Need to Know" basis only. **Examples** include employee personal information, business plans, unpublished financial statements, etc.
VERY HIGH	HIGHLY CONFIDENTIAL	**HIGHLY CONFIDENTIAL INFORMATION** Highly confidential information is the most sensitive form of information. It is so sensitive that disclosure or usage would have a definite impact on ABC's business and future and / or national security of the located Country. Extremely restrictive controls need to be applied (e.g., very limited audience). **Examples** include strategic plans, investment decisions etc.



RISK RATING	CLASSIFICATION	IMPACT
Very Low	Non critical	No impact. Asset can be easily replaced. These assets may be interrupted for an extended period of time, at little or no cost to the company, and require little or no catching up when restored.
Low	Sensitive	Unavailability of the asset will not significantly affect ABC's operations and services. Asset can be replaced within an acceptable timeframe without significantly affecting operations. Manual processes at a tolerable cost can replace these assets for an extended period of time. While they can be performed manually it is usually a difficult process and requires additional staff to perform.
Medium	Vital	Unavailability of the asset will not significantly affect ABC's operations and services. These assets can be replaced by manual processes - but only for a brief period of time. There is a higher tolerance to interruption than with critical and highly critical systems and therefore somewhat lower costs of interruption provided that functions are restored within a certain timeframe. (***Usually 5 days or less***)
High	Critical	Unavailability of the asset will affect **individual** operations and services. These assets cannot be operated unless they are replaced by **identical or similar** capabilities. Critical assets cannot be replaced by manual methods. Tolerance to interruption is **LOW**; therefore cost to interruption is **HIGH.**
Very High	Highly Critical	Unavailability of the asset for any time frame will significantly affect **multiple** operations and services. These assets cannot be operated unless they are replaced by **identical** capabilities. Highly critical assets cannot be replaced by manual methods. Tolerance to interruption is **VERY LOW**; therefore cost to interruption is **VERY HIGH.**

Develop the Threat Model based on the ISO/IEC 27004 requirement

- In risk assessment methods of this type, actual or proposed physical assets are valued in terms of replacement or reconstruction costs (i.e. quantitative measurements). These costs are then converted onto the same qualitative scale as that used for information (see below). Actual or proposed software assets are valued in the same way as physical assets, with purchase or reconstruction costs identified and then converted to the same qualitative scale as that used for information. Additionally, if any application software is found to have its own intrinsic requirements for confidentiality or integrity (for example if source code is itself commercially sensitive), it is valued in the same way as for information.
- The values for information are obtained by interviewing selected business management (the “data owners”) who can speak authoritatively about the data, to determine the value and sensitivity of the data actually in use, or to be stored, processed or accessed. The interviews facilitate assessment of the value and sensitivity of the information in terms of the worst case scenarios that could be reasonably expected to happen from adverse business consequences due to unauthorized disclosure, unauthorized modification, non-availability for varying time periods, and destruction.
- The valuation is accomplished using information valuation guidelines, which cover such issues as:
  - Personal safety
    - ***Personal information***
    - ***Legal and regulatory obligations***
    - ***Law enforcement***
    - ***Commercial and economic interests***
    - ***Financial loss/disruption of activities***
    - ***Public order***
    - ***Business policy and operations***
    - ***Loss of goodwill***
    - ***Contract or agreement with a customer***
- The guidelines facilitate identification of the values on a numeric scale, such as the 0 to 4 scale shown in the example matrix below, thus enabling the recognition of quantitative values where possible and logical, and qualitative values where quantitative values are not possible, e.g. for endangerment of human life.



Standard Risk Matrix

12

IMPACT

High impact, Low probability risks
Low probability (below 50%)
High impact (8 and above)

High impact, High probability risks
High probability (above 50%)
High impact (8 and above)

PROBABILITY

0%

100%

PROBABILITY

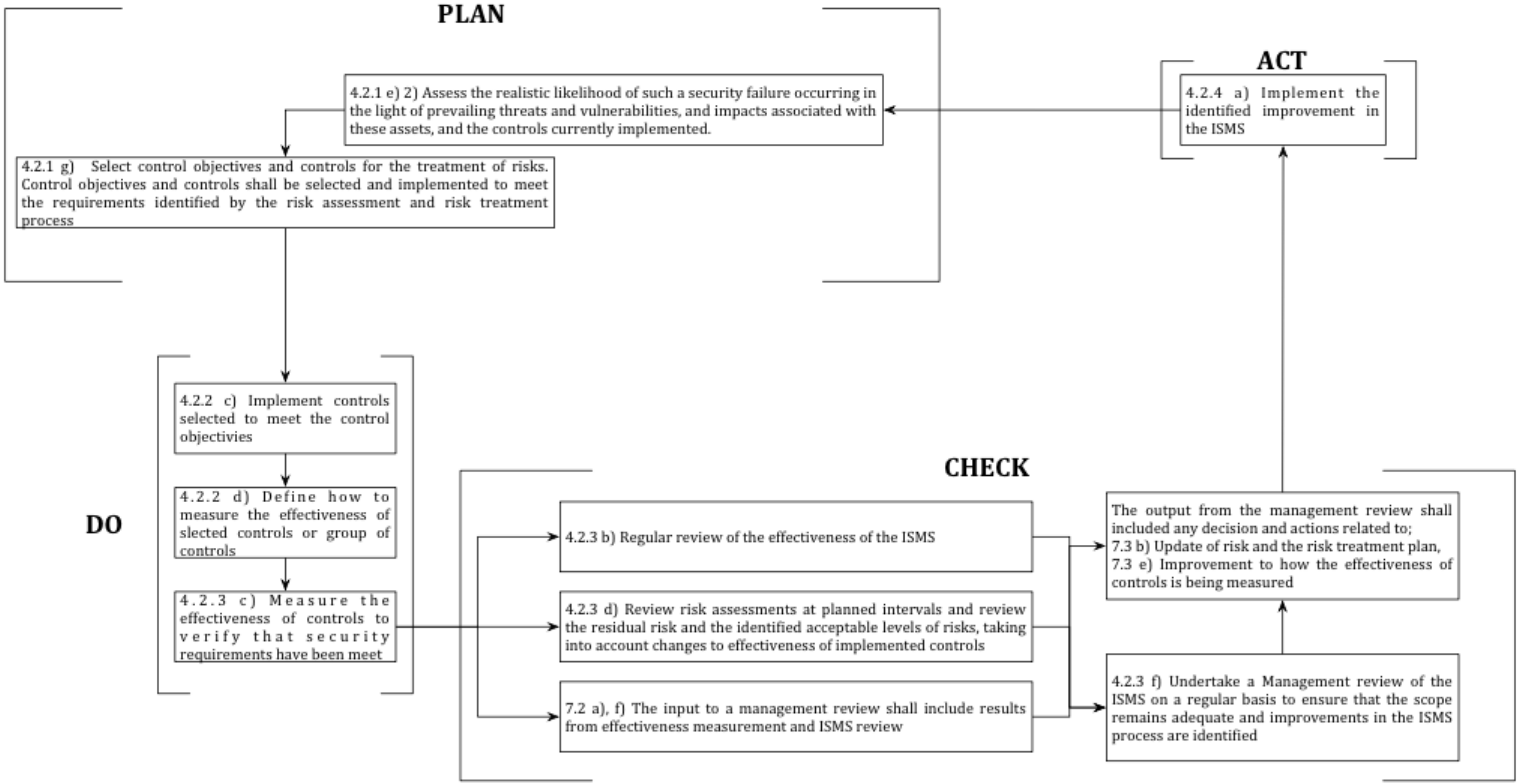
Low impact, Low probability risks
Low probability (below 50%)
Low impact (below 8)

Low impact, High probability risks
High probability (above 50%)
Low impact (below 8)

IMPACT

4

Develop the Threat Model based on the ISO/IEC 27004 requirement



PLAN

4.2.1 e) 2) Assess the realistic likelihood of such a security failure occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented.

4.2.1 g) Select control objectives and controls for the treatment of risks. Control objectives and controls shall be selected and implemented to meet the requirements identified by the risk assessment and risk treatment process

DO

4.2.2 c) Implement controls selected to meet the control objectivies

4.2.2 d) Define how to measure the effectiveness of slected controls or group of controls

4.2.3 c) Measure the effectiveness of controls to verify that security requirements have been meet

CHECK

4.2.3 b) Regular review of the effectiveness of the ISMS

4.2.3 d) Review risk assessments at planned intervals and review the residual risk and the identified acceptable levels of risks, taking into account changes to effectiveness of implemented controls

7.2 a), f) The input to a management review shall include results from effectiveness measurement and ISMS review

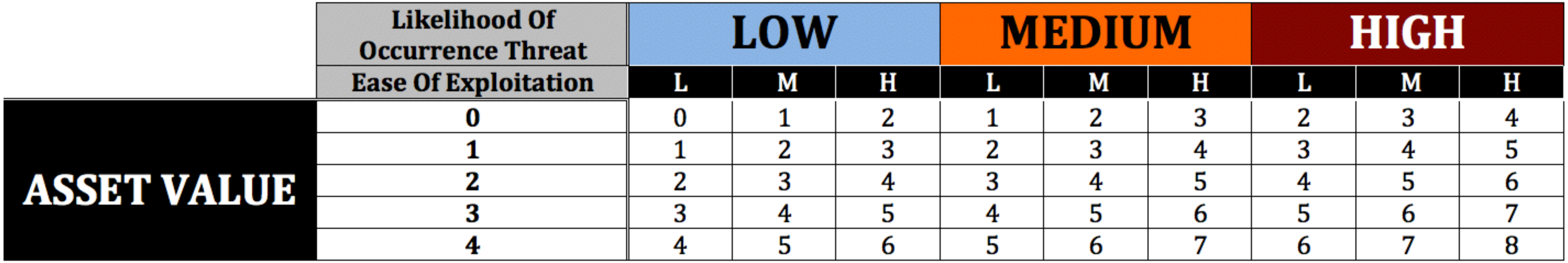
The output from the management review shall included any decision and actions related to;
7.3 b) Update of risk and the risk treatment plan,
7.3 e) Improvement to how the effectiveness of controls is being measured

4.2.3 f) Undertake a Management review of the ISMS on a regular basis to ensure that the scope remains adequate and improvements in the ISMS process are identified

ACT

4.2.4 a) Implement the identified improvement in the ISMS

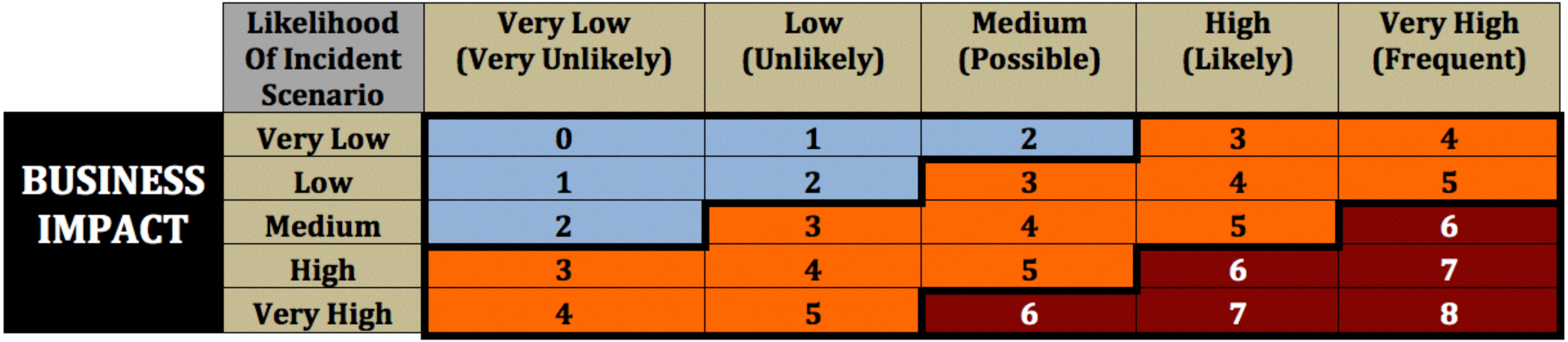
Develop the Threat Model based on the ISO/IEC 27004 requirement



	Likelihood Of Occurrence Threat	LOW			MEDIUM			HIGH		
	Ease Of Exploitation	L	M	H	L	M	H	L	M	H
ASSET VALUE	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

- For each asset, the relevant vulnerabilities and their corresponding threats are considered. If there is a vulnerability without a corresponding threat, or a threat without corresponding vulnerability, there is presently no risk (but care should be taken in case this situation changes). Now the appropriate row in the matrix is identified by the asset value, and the appropriate column is identified by the likelihood of the threat occurring and the ease of exploitation. For example, if the asset has the **value 3**, the threat is “**high**” and the vulnerability “**low**”, the measure of **risk is 5**. Assume an asset has a **value of 2**, e.g. for modification, the threat level is “**low**” and the ease of exploitation is “**high**”, then the measure of **risk is 4**. The size of the matrix, in terms of the number of threat likelihood categories, ease of exploitation categories and the number of asset valuation categories, can be adjusted to the needs of the organization. Additional columns and rows will necessitate additional risk measures. The value of this approach is in ranking the risks to be addressed.

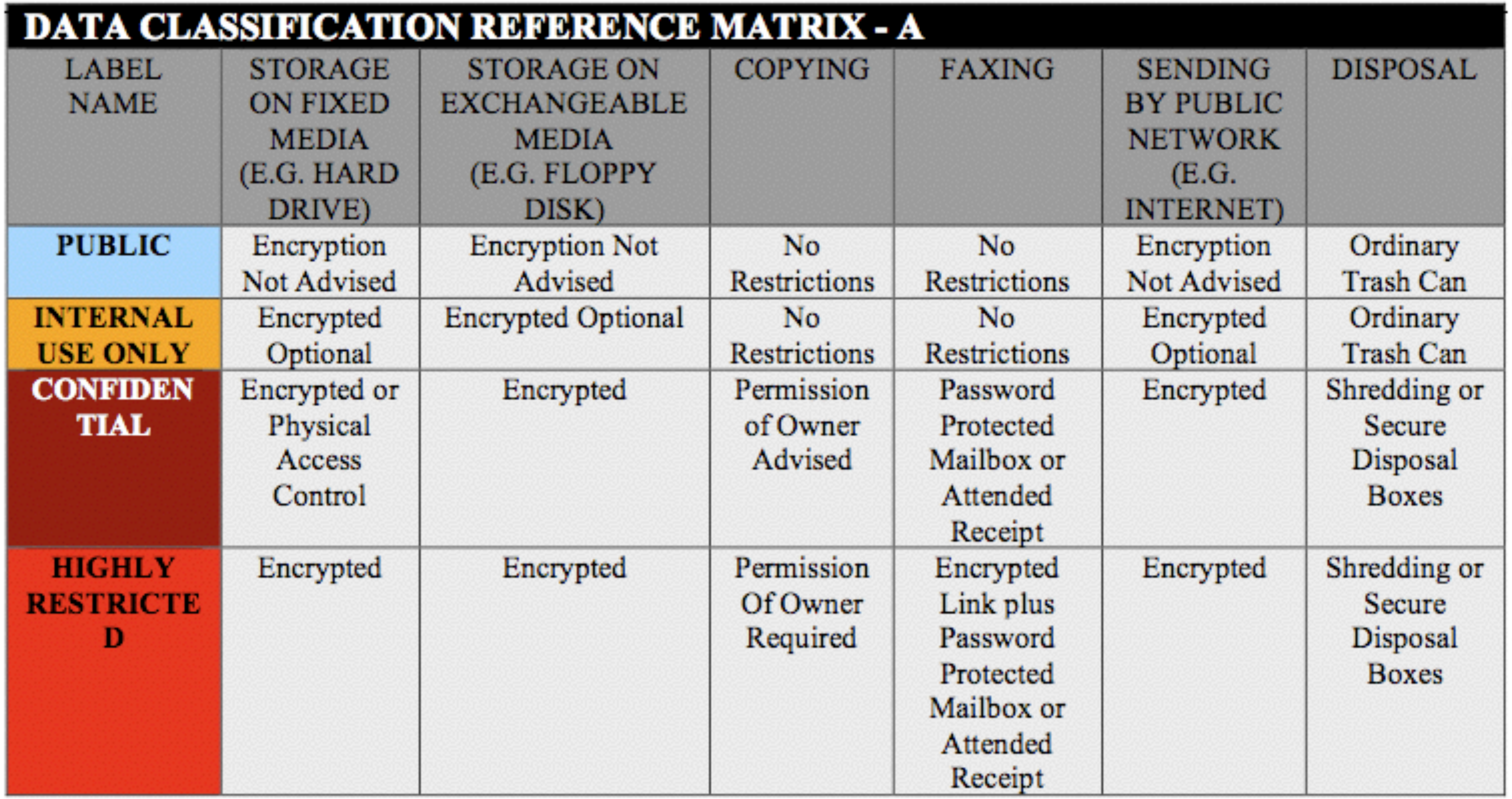
Develop the Threat Model based on the ISO/IEC 27004 requirement



	Likelihood Of Incident Scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
BUSINESS IMPACT	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

- A similar Matrix as shown in pervious table results from the consideration of the likelihood of an incident scenario, mapped against the estimated business impact. The likelihood of an incident scenario is given by a threat exploiting a vulnerability with a certain likelihood. The Table maps this likelihood against the business impact related to the incident scenario. The resulting risk is measured on a scale of 0 to 8 that can be evaluated against risk acceptance criteria. This risk scale could also be mapped to a simple overall risk rating, for example as:
    - Low risk: 0-2
    - Medium Risk: 3-5
    - High Risk:6-8

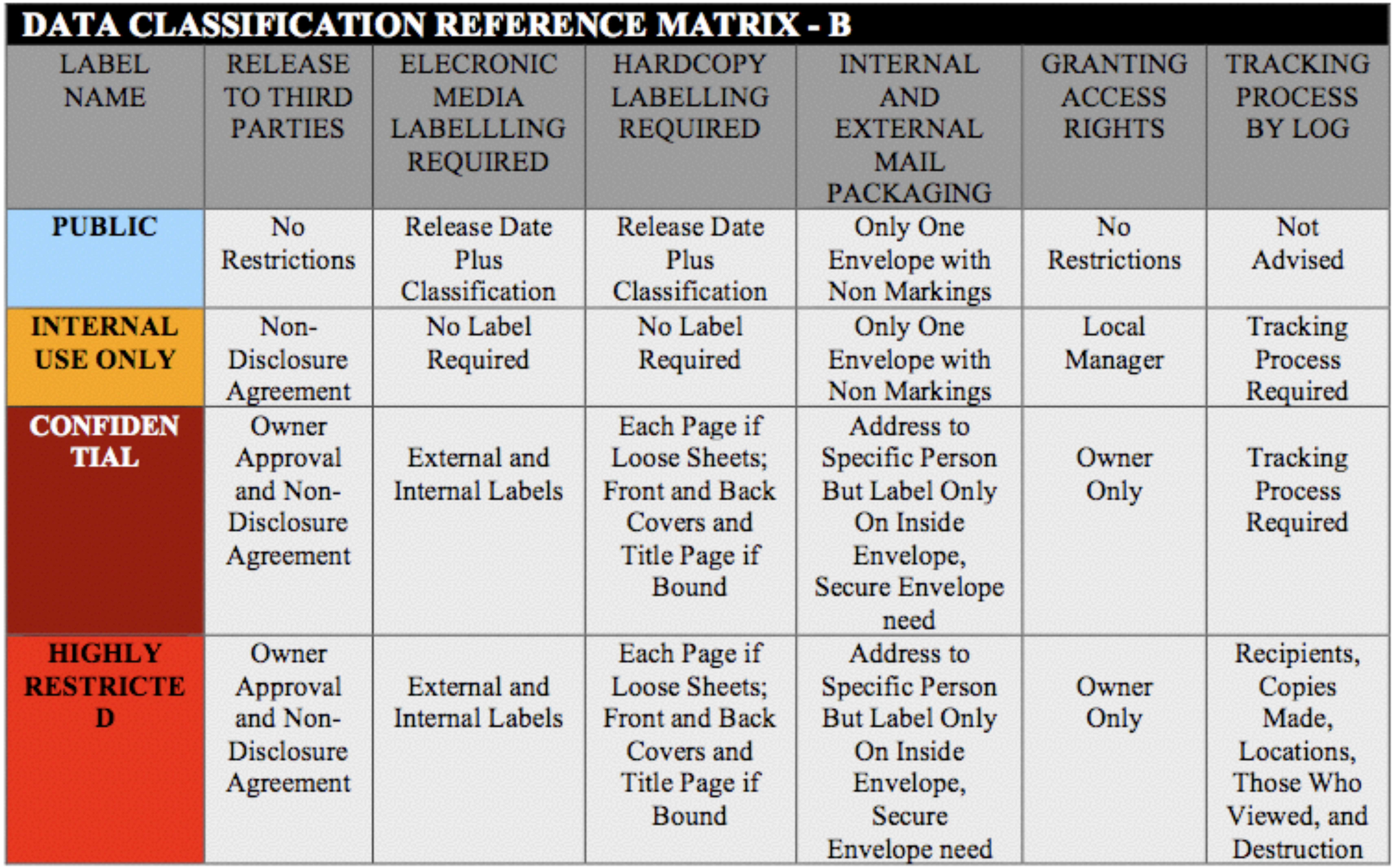
Develop the Threat Model based on the ISO/IEC 27004 requirement



DATA CLASSIFICATION REFERENCE MATRIX - A

LABEL NAME	STORAGE ON FIXED MEDIA (E.G. HARD DRIVE)	STORAGE ON EXCHANGEABLE MEDIA (E.G. FLOPPY DISK)	COPYING	FAXING	SENDING BY PUBLIC NETWORK (E.G. INTERNET)	DISPOSAL
PUBLIC	Encryption Not Advised	Encryption Not Advised	No Restrictions	No Restrictions	Encryption Not Advised	Ordinary Trash Can
INTERNAL USE ONLY	Encrypted Optional	Encrypted Optional	No Restrictions	No Restrictions	Encrypted Optional	Ordinary Trash Can
CONFIDENTIAL	Encrypted or Physical Access Control	Encrypted	Permission of Owner Advised	Password Protected Mailbox or Attended Receipt	Encrypted	Shredding or Secure Disposal Boxes
HIGHLY RESTRICTED	Encrypted	Encrypted	Permission Of Owner Required	Encrypted Link plus Password Protected Mailbox or Attended Receipt	Encrypted	Shredding or Secure Disposal Boxes

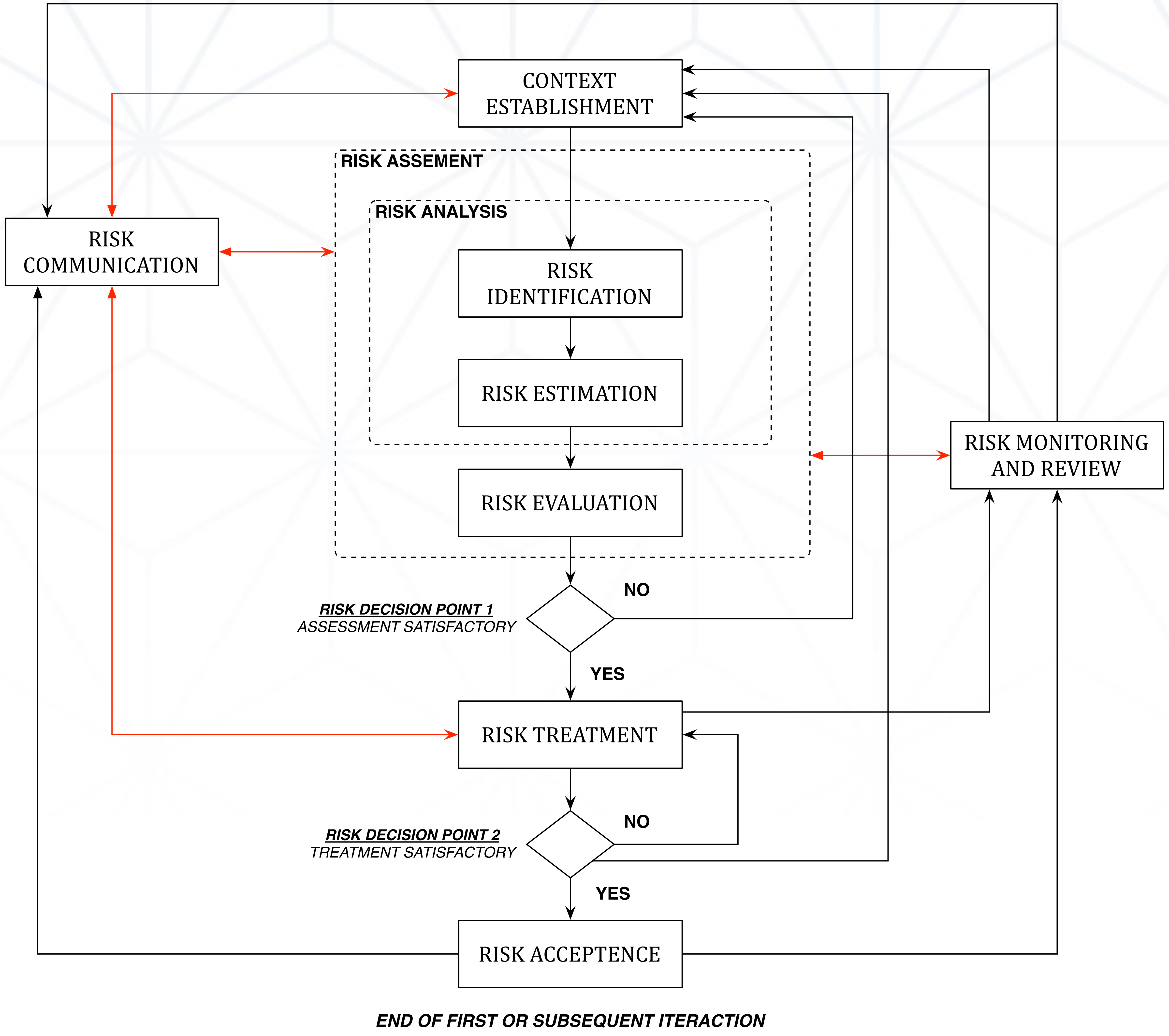
Develop the Threat Model based on the ISO/IEC 27004 requirement



DATA CLASSIFICATION REFERENCE MATRIX - B

LABEL NAME	RELEASE TO THIRD PARTIES	ELECRONIC MEDIA LABELLLING REQUIRED	HARDCOPY LABELLING REQUIRED	INTERNAL AND EXTERNAL MAIL PACKAGING	GRANTING ACCESS RIGHTS	TRACKING PROCESS BY LOG
PUBLIC	No Restrictions	Release Date Plus Classification	Release Date Plus Classification	Only One Envelope with Non Markings	No Restrictions	Not Advised
INTERNAL USE ONLY	Non-Disclosure Agreement	No Label Required	No Label Required	Only One Envelope with Non Markings	Local Manager	Tracking Process Required
CONFIDEN TIAL	Owner Approval and Non-Disclosure Agreement	External and Internal Labels	Each Page if Loose Sheets; Front and Back Covers and Title Page if Bound	Address to Specific Person But Label Only On Inside Envelope, Secure Envelope need	Owner Only	Tracking Process Required
HIGHLY RESTRICTE D	Owner Approval and Non-Disclosure Agreement	External and Internal Labels	Each Page if Loose Sheets; Front and Back Covers and Title Page if Bound	Address to Specific Person But Label Only On Inside Envelope, Secure Envelope need	Owner Only	Recipients, Copies Made, Locations, Those Who Viewed, and Destruction

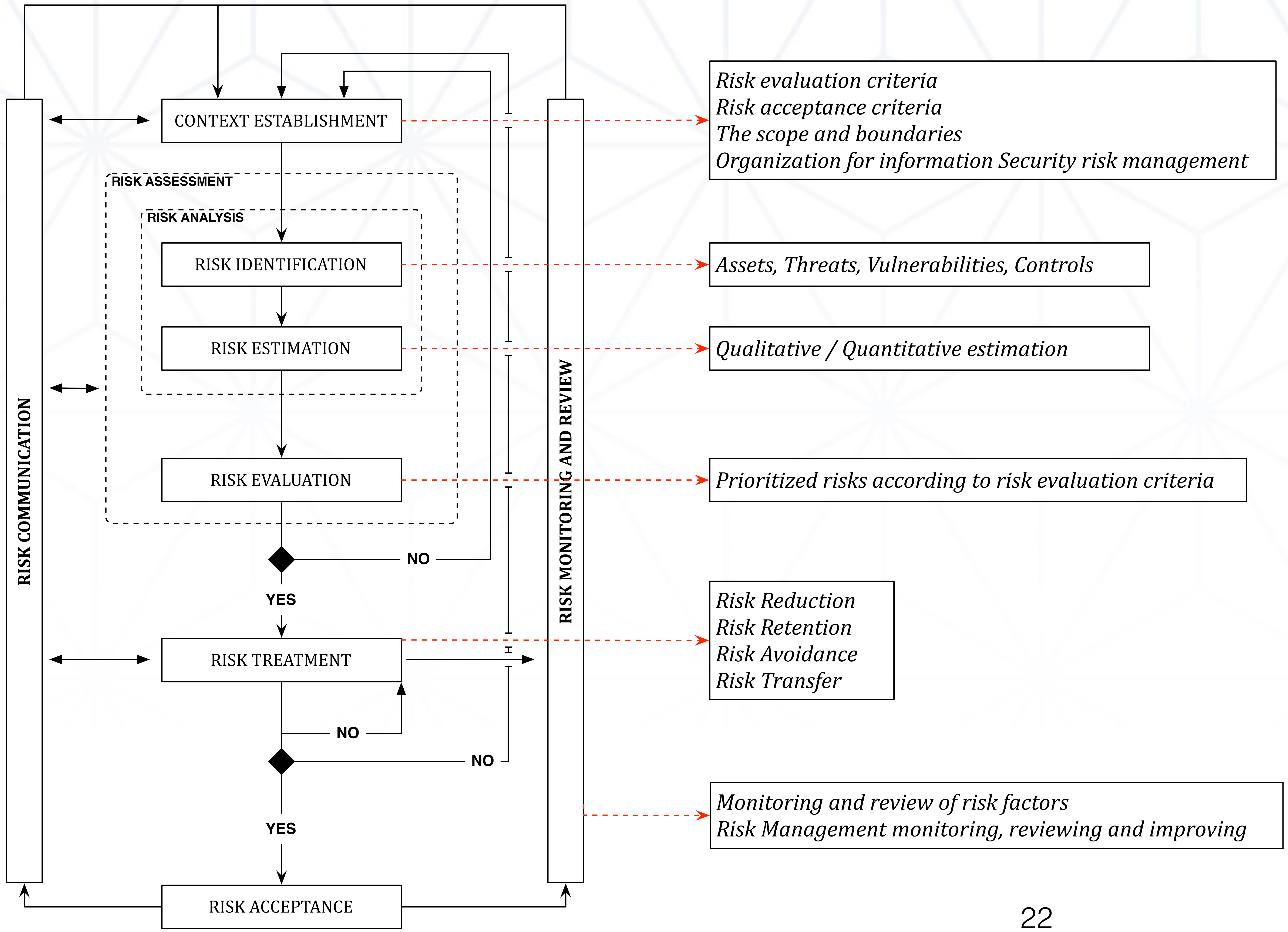
Develop the Threat Model based on the ISO/IEC 27004 requirement with 27005 Risk Assessment Method



Impact criteria

- Impact criteria should be developed and specified in terms of the degree of damage or costs to the organization caused by an information security event considering the following:
  - *Level of classification of the impacted information asset*
  - *Breaches of information security (e.g. loss of confidentiality, integrity and availability) Impaired operations (internal or third parties)*
  - *Loss of business and financial value*
  - *Disruption of plans and deadlines*
  - *Damage of reputation*
  - *Breaches of legal, regulatory or contractual requirements*
- NOTE See also ISO/IEC 27001 [Clause 4.2.1 d) 4] concerning the impact criteria identification for losses of confidentiality, integrity and availability.

Develop the Threat Model based on the ISO/IEC 27004 requirement with 27005 Risk Assessment Method



RISK COMMUNICATION

CONTEXT ESTABLISHMENT

RISK ASSESSMENT

RISK ANALYSIS

RISK IDENTIFICATION

RISK ESTIMATION

RISK EVALUATION

NO

YES

RISK TREATMENT

NO

NO

YES

RISK ACCEPTANCE

RISK MONITORING AND REVIEW

Risk evaluation criteria
Risk acceptance criteria
The scope and boundaries
Organization for information Security risk management

Assets, Threats, Vulnerabilities, Controls

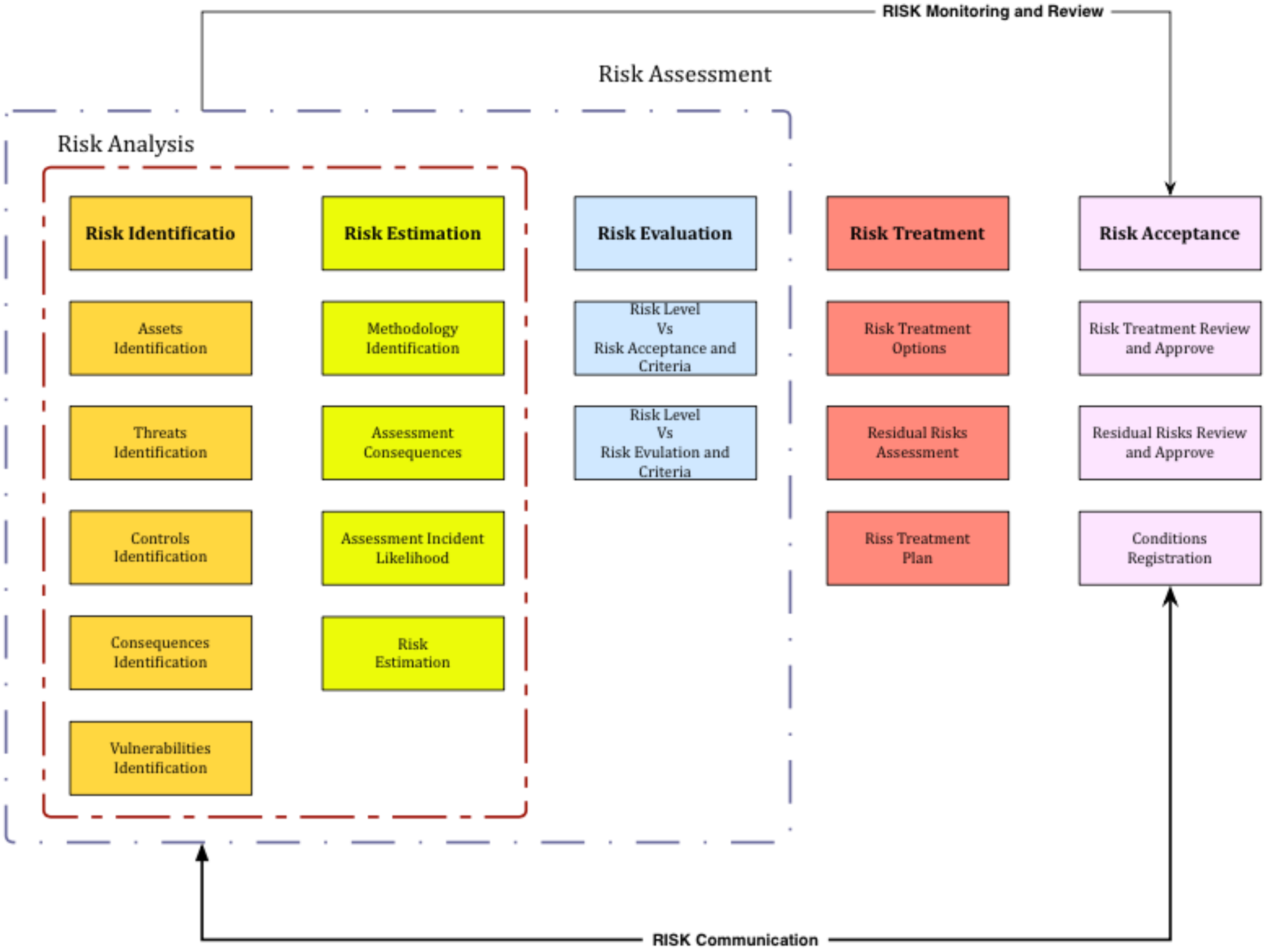
Qualitative / Quantitative estimation

Prioritized risks according to risk evaluation criteria

Risk Reduction
Risk Retention
Risk Avoidance
Risk Transfer

Monitoring and review of risk factors
Risk Management monitoring, reviewing and improving

Develop the Threat Model based on the ISO/IEC 27004 requirement with 27005 Risk Assessment Method



RISK Monitoring and Review

Risk Assessment

Risk Analysis

Risk Identificatio	Risk Estimation	Risk Evaluation	Risk Treatment	Risk Acceptance
Assets Identification	Methodology Identification	Risk Level Vs Risk Acceptance and Criteria	Risk Treatment Options	Risk Treatment Review and Approve
Threats Identification	Assessment Consequences	Risk Level Vs Risk Evulation and Criteria	Residual Risks Assessment	Residual Risks Review and Approve
Controls Identification	Assessment Incident Likelihood		Riss Treatment Plan	Conditions Registration
Consequences Identification	Risk Estimation			
Vulnerabilities Identification				

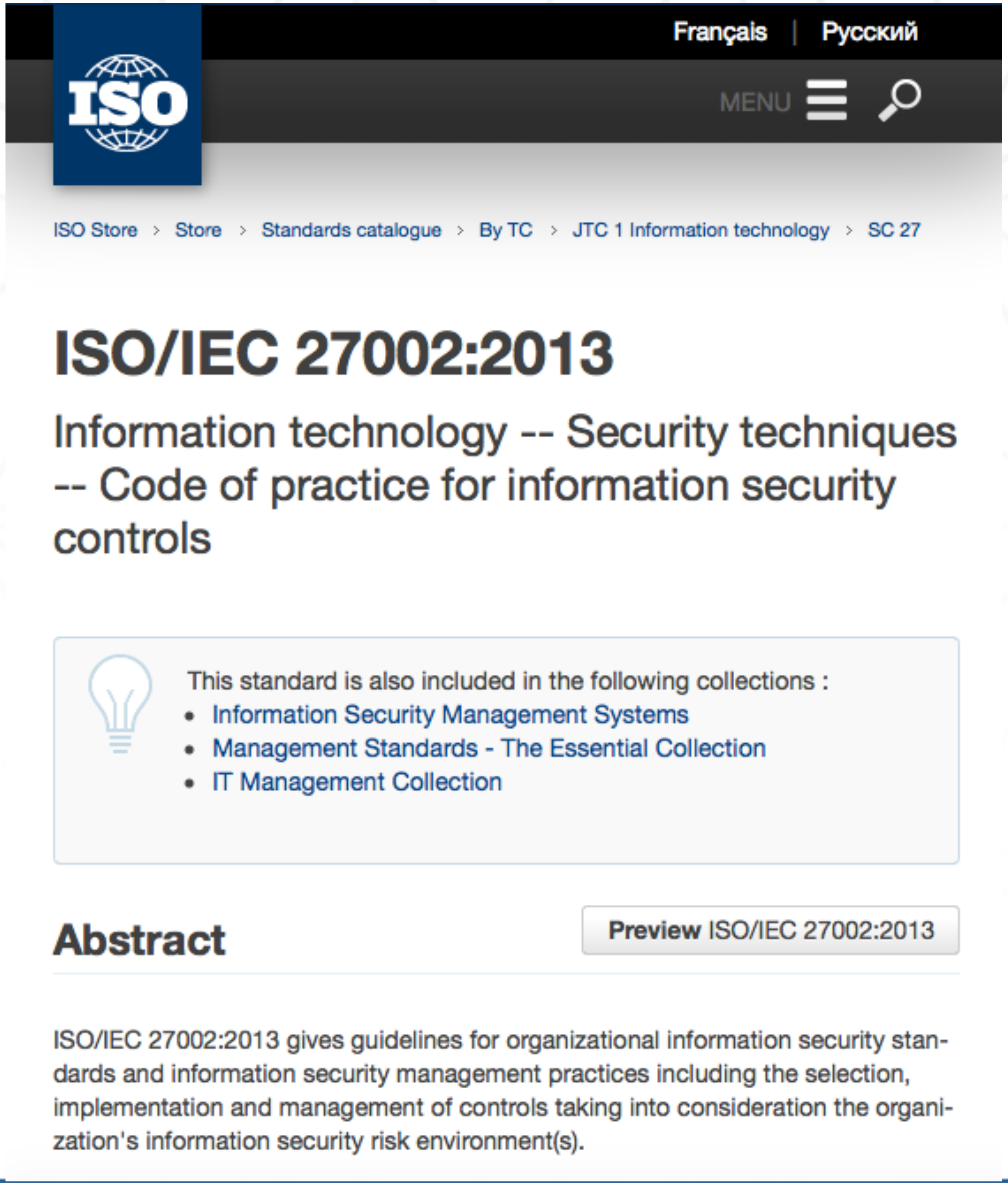
RISK Communication

Develop the Threat Model based on the ISO/IEC 27004 requirement

Risk acceptance criteria

- Risk acceptance criteria should be developed and specified. Risk acceptance criteria often depend on the organization's policies, goals, objectives and the interests of stakeholders. An organization should define its own scales for levels of risk acceptance. The following should be considered during development:
  - *Risk acceptance criteria may include multiple thresholds, with a desired target level of risk, but provision for senior managers to accept risks above this level under defined circumstances*
  - *Risk acceptance criteria may be expressed as the ratio of estimated profit (or other business benefit) to the estimated risk*
  - *Different risk acceptance criteria may apply to different classes of risk, e.g. risks that could result in non- compliance with regulations or laws may not be accepted, while acceptance of high risks may be allowed if this is specified as a contractual requirement*
  - *Risk acceptance criteria may include requirements for future additional treatment, e.g. a risk may be accepted if there is approval and commitment to take action to reduce it to an acceptable level within a defined time period*
- Risk acceptance criteria may differ according to how long the risk is expected to exist, e.g. the risk may be associated with a temporary or short term activity. Risk acceptance criteria should be set up considering the following:
  - *Business criteria*
  - *Legal and regulatory aspects*
  - *Operations*
  - *Technology*
  - *Finance*
  - *Social and humanitarian factors*
- **NOTE:** Risk acceptance criteria correspond to “criteria for accepting risks and identify the acceptable level of risk”specified in ISO/IEC 27001 Clause 4.2.1 c) 2).

How about 27002 and 27003 ?



ISO Store > Store > Standards catalogue > By TC > JTC 1 Information technology > SC 27

ISO/IEC 27002:2013

Information technology -- Security techniques -- Code of practice for information security controls

This standard is also included in the following collections :

- Information Security Management Systems
- Management Standards - The Essential Collection
- IT Management Collection

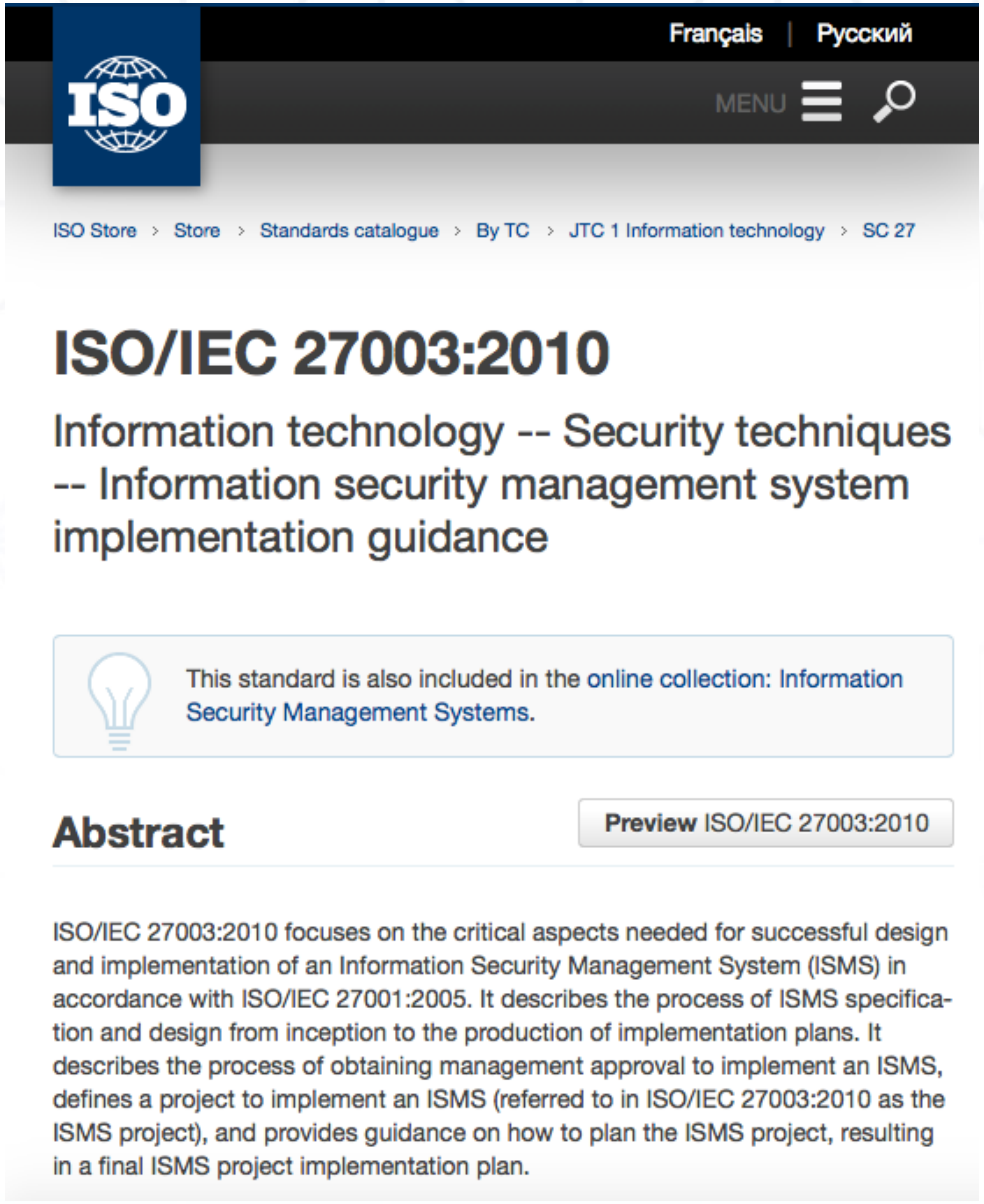
Abstract

Preview ISO/IEC 27002:2013

ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

- **How to establish security requirements**
  - It is essential that an organisation identifies its security requirements. There are three main sources of security requirements.
    1. *One source is derived from assessing risks to the organisation, taking into account the organisation's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potentialimpact is estimated.*
    2. *Another source is the legal, statutory, regulatory, and contractual requirements that an organisation, its trading partners, contractors, and service providers have to satisfy, and their socio-cultural environment.*
    3. *A further source is the particular set of principles, objectives and business requirements for information processing that an organisation has developed to support its operations.*
- **Assessing security risks**
  - Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business harm likely to result from security failures.
  - The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.
  - Risk assessment should be repeated periodically to address any changes that might influence the risk assessment results. More information about the assessment of security risks can be found in clause 4.1 "Assessing security risks".

How about 27002 and 27003 ?


Français | Русский
MENU
ISO Store › Store › Standards catalogue › By TC › JTC 1 Information technology › SC 27

ISO/IEC 27003:2010

Information technology -- Security techniques -- Information security management system implementation guidance

This standard is also included in the online collection: Information Security Management Systems.

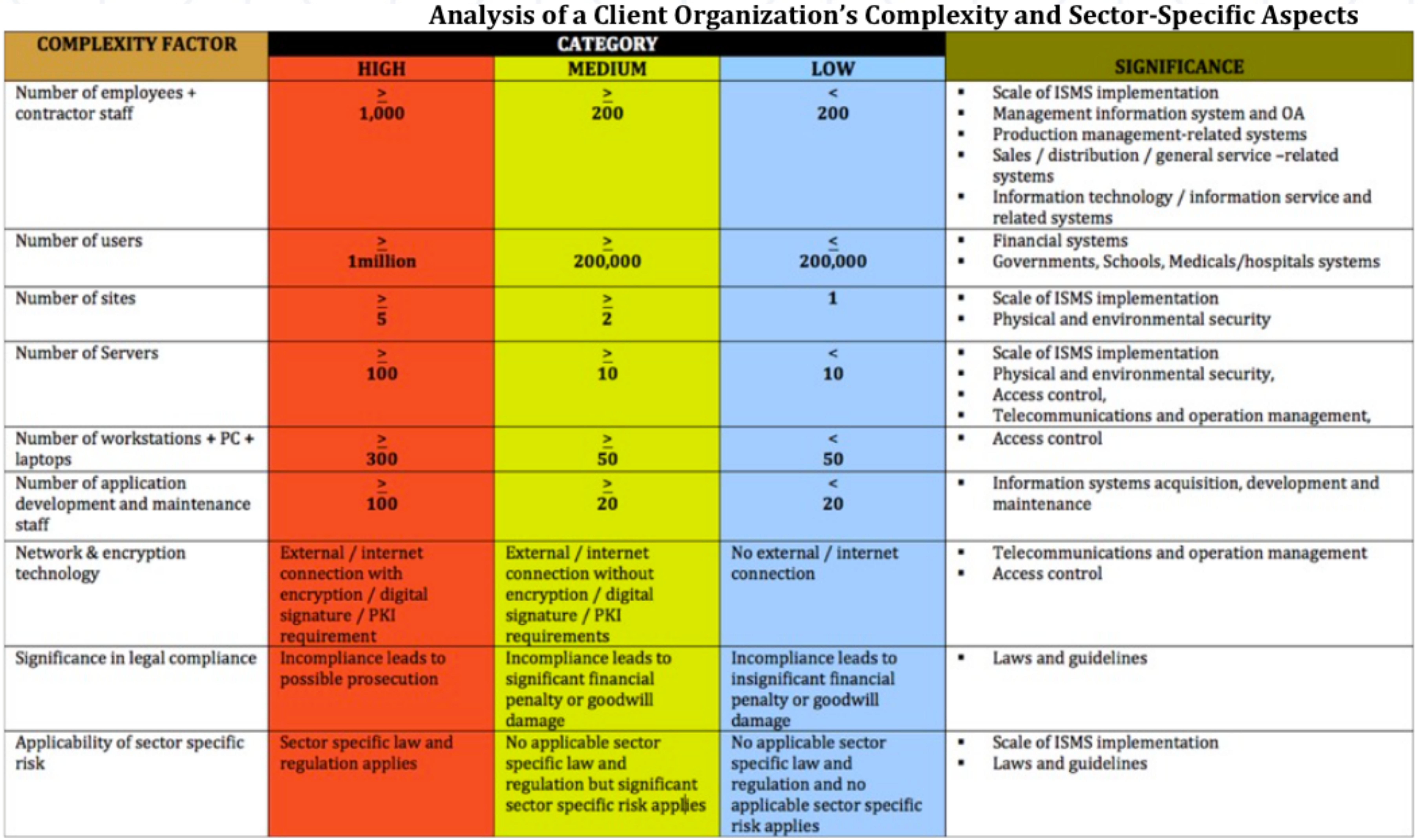
Abstract

Preview ISO/IEC 27003:2010

ISO/IEC 27003:2010 focuses on the critical aspects needed for successful design and implementation of an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2005. It describes the process of ISMS specification and design from inception to the production of implementation plans. It describes the process of obtaining management approval to implement an ISMS, defines a project to implement an ISMS (referred to in ISO/IEC 27003:2010 as the ISMS project), and provides guidance on how to plan the ISMS project, resulting in a final ISMS project implementation plan.

- **Selecting controls**
  - Once security requirements and risks have been identified and decisions for the treatment of risks have been made, appropriate controls should be selected and implemented to ensure risks are reduced to an acceptable level. Controls can be selected from this standard or from other control sets, or new controls can be designed to meet specific needs as appropriate. The selection of security controls is dependent upon organisational decisions based on the criteria for risk acceptance, risk treatment options, and the general risk management approach applied to the organisation, and should also be subject to all relevant national and international legislation and regulations.
  - Some of the controls in this standard can be considered as guiding principles for information security management and applicable for most organisations. They are explained in more detail below under the heading “Information security starting point”.
  - More information about selecting controls and other risk treatment options can be found in clause 4.2 "Treating security risks".

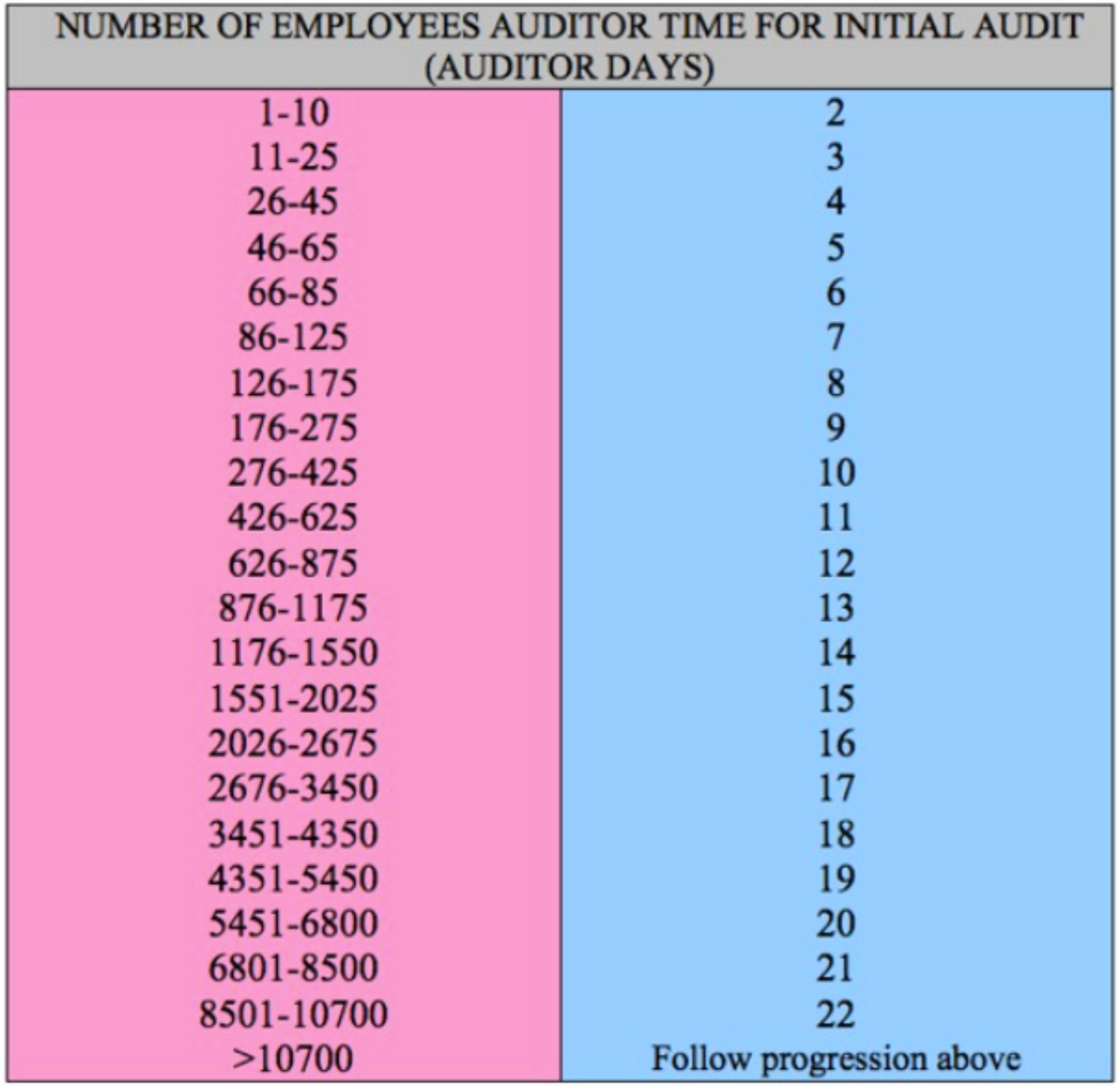
How about 27006 and 27007?



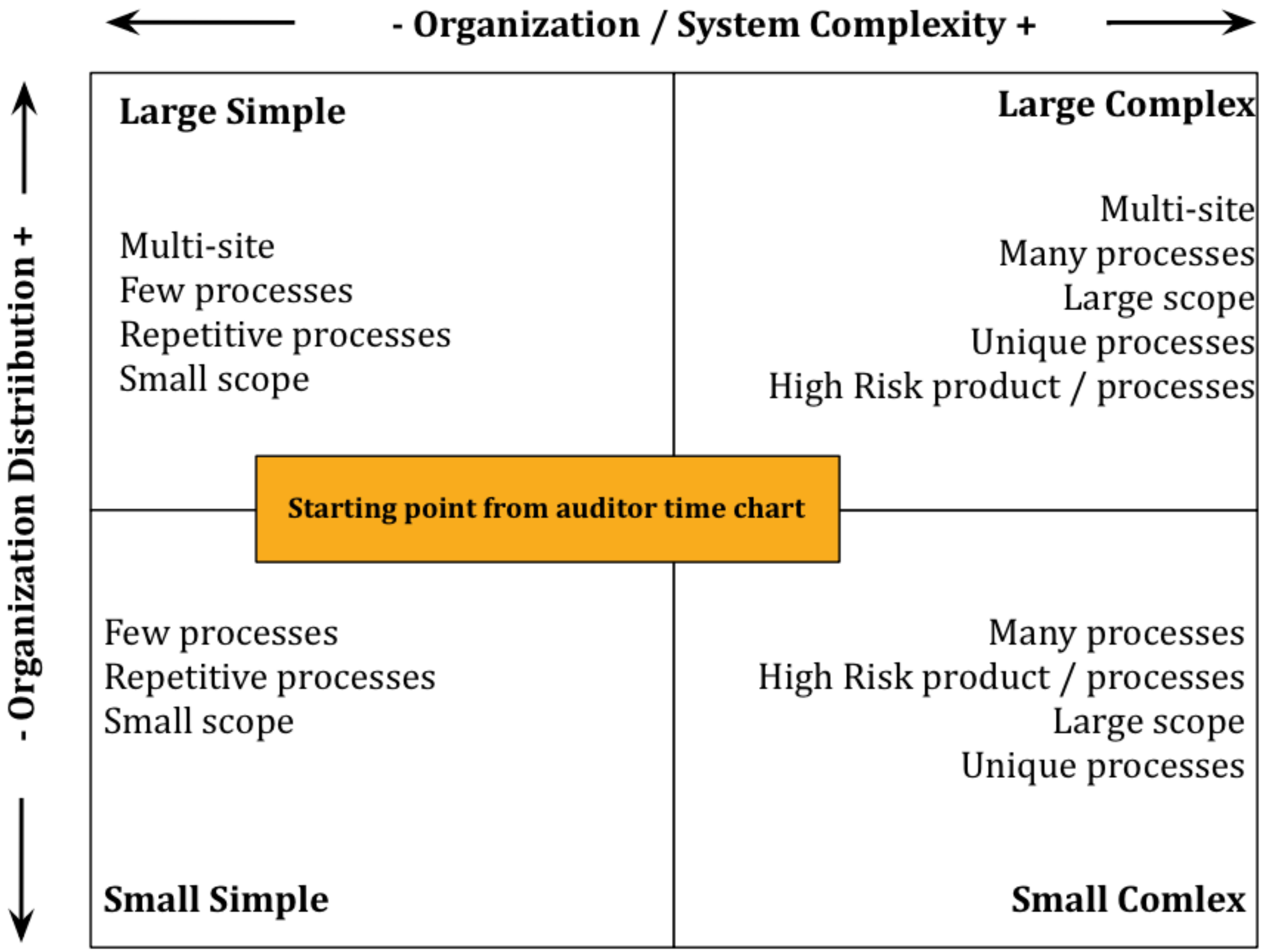
Analysis of a Client Organization's Complexity and Sector-Specific Aspects

COMPLEXITY FACTOR	CATEGORY			SIGNIFICANCE
	HIGH	MEDIUM	LOW	
Number of employees + contractor staff	≥ 1,000	≥ 200	< 200	▪ Scale of ISMS implementation ▪ Management information system and OA ▪ Production management-related systems ▪ Sales / distribution / general service –related systems ▪ Information technology / information service and related systems
Number of users	≥ 1million	≥ 200,000	≤ 200,000	▪ Financial systems ▪ Governments, Schools, Medicals/hospitals systems
Number of sites	≥ 5	≥ 2	1	▪ Scale of ISMS implementation ▪ Physical and environmental security
Number of Servers	≥ 100	≥ 10	< 10	▪ Scale of ISMS implementation ▪ Physical and environmental security, ▪ Access control, ▪ Telecommunications and operation management,
Number of workstations + PC + laptops	≥ 300	≥ 50	< 50	▪ Access control
Number of application development and maintenance staff	≥ 100	≥ 20	< 20	▪ Information systems acquisition, development and maintenance
Network & encryption technology	External / internet connection with encryption / digital signature / PKI requirement	External / internet connection without encryption / digital signature / PKI requirements	No external / internet connection	▪ Telecommunications and operation management ▪ Access control
Significance in legal compliance	Incompliance leads to possible prosecution	Incompliance leads to significant financial penalty or goodwill damage	Incompliance leads to insignificant financial penalty or goodwill damage	▪ Laws and guidelines
Applicability of sector specific risk	Sector specific law and regulation applies	No applicable sector specific law and regulation but significant sector specific risk applies	No applicable sector specific law and regulation and no applicable sector specific risk applies	▪ Scale of ISMS implementation ▪ Laws and guidelines

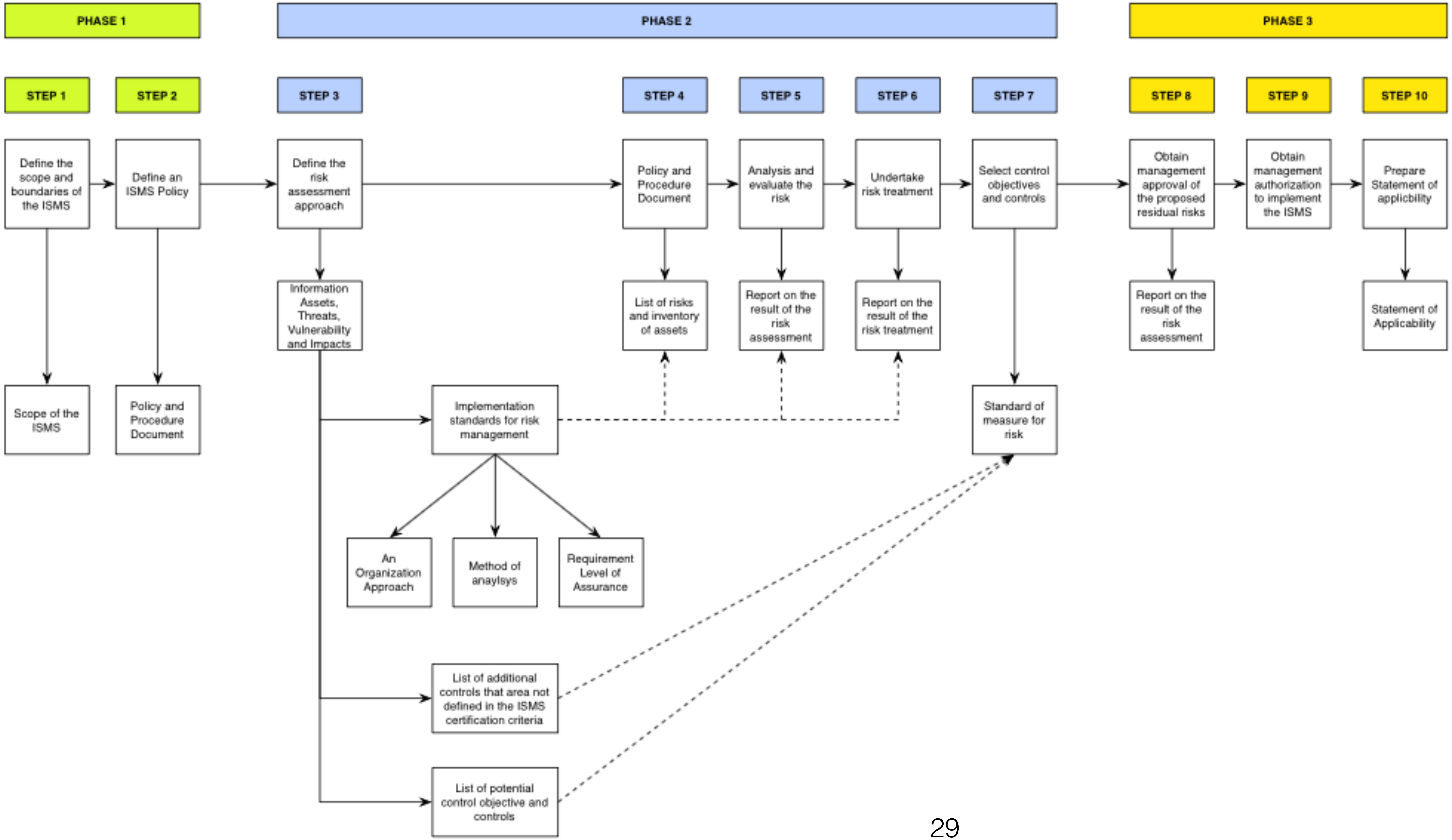
How about 27006 and 27007?



NUMBER OF EMPLOYEES	AUDITOR TIME FOR INITIAL AUDIT (AUDITOR DAYS)
1-10	2
11-25	3
26-45	4
46-65	5
66-85	6
86-125	7
126-175	8
176-275	9
276-425	10
426-625	11
626-875	12
876-1175	13
1176-1550	14
1551-2025	15
2026-2675	16
2676-3450	17
3451-4350	18
4351-5450	19
5451-6800	20
6801-8500	21
8501-10700	22
>10700	Follow progression above



How about 27006 and 27007?



PHASE 1

STEP 1

Define the scope and boundaries of the ISMS

Scope of the ISMS

STEP 2

Define an ISMS Policy

Policy and Procedure Document

PHASE 2

STEP 3

Define the risk assessment approach

Information Assets, Threats, Vulnerability and Impacts

Implementation standards for risk management

An Organization Approach

Method of anaylsys

Requirement Level of Assurance

List of additional controls that area not defined in the ISMS certification criteria

List of potential control objective and controls

STEP 4

Policy and Procedure Document

List of risks and inventory of assets

STEP 5

Analysis and evaluate the risk

Report on the result of the risk assessment

STEP 6

Undertake risk treatment

Report on the result of the risk treatment

STEP 7

Select control objectives and controls

Standard of measure for risk

PHASE 3

STEP 8

Obtain management approval of the proposed residual risks

Report on the result of the risk assessment

STEP 9

Obtain management authorization to implement the ISMS

STEP 10

Prepare Statement of applicbility

Statement of Applicability

Q&A