



Information Security Governance In Practise



Who am i

Peter Houtmeyers

CISA, CISM, CGEIT, CISSP, ISO27001 Lead auditor

Email : p.houtmeyers@branswijk.com

Phone : +32474 45 37 04



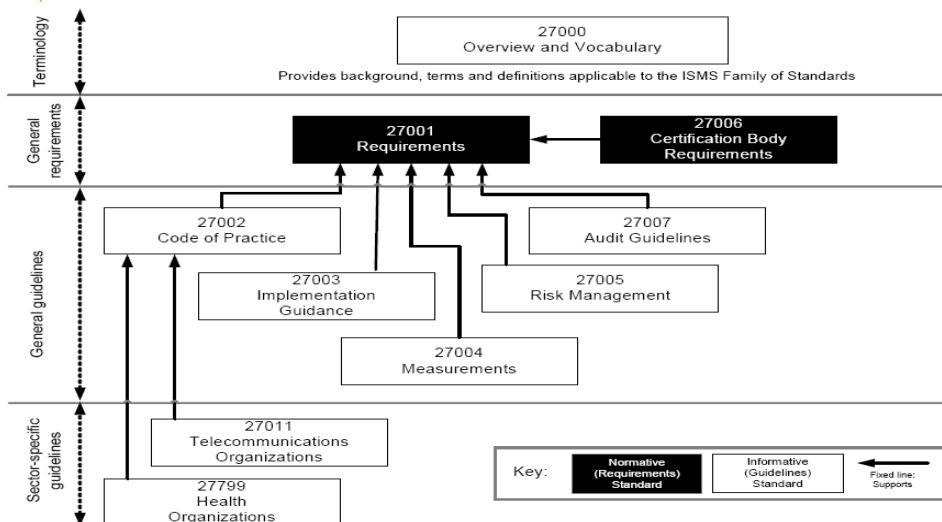


What is information

“Information is an **asset** which, like other important business assets, has **value** to an organization and consequently needs to be **suitably protected**.”



The 27000 family





Major drivers

- Reduce frequency and impact of major incidents
- Implement best practice
- Evaluate the status of controls
- Meet regulatory requirements



Important drivers

- Maximise existing investment
- Comply with internal policy
- Integrate into a risk management programme





Other drivers

- Gain competitive advantage
- Respond to pressure from third parties
- Achieve cost savings
- Security management



Implementing a good standard

Helps you to :

- Move towards international best practice
- Manage information risk
- Build confidence towards third parties that information security is being addressed in a professional manner
- Reduce the likelihood of disruption from major incidents
- Fight the emerging threats of cyber crime
- Comply with legal and regulatory requirements
- Maintain business integrity



Shift in IS perspective

From :

- Security is a technical problem
- Security has a technical owner
- There is an explicit focus on security
- Security is an expense
- The goal is security



Shift in IS perspective

TO :

- Security is an enterprise-wide problem
- Security is owned by the business
- Security is transparent
- Security is an investment
- The goal is business continuity and ultimately resiliency





CASE example



Assignment

- The company wants to create proper Information Security Management System (ISMS) to benefit from the model. The approach must be process driven to fine-tune the IT security governance model and to obtain buy-in of the stakeholders.
- The company wants to have assistance in the definition of a pragmatic process leading to ISO 27001 certification.





Assignment

- The assistance focus on 2 main topics:
 - IT Security Governance (ISO27001) AS-IS
 - IT Security Governance (ISO27001) TO-BE roadmap



Maturity assessment groups

- Legal
- Risk Manager and Quality assurance
- Physical Security Officer
- IT Project Manager
- Human Resources
- Helpdesk and asset manager
- Network operations
- IT security officer
- Application development manager
- CIO and IT manager



Maturity assessment scale

- **0 Non-existent.**
 - Complete lack of any recognizable processes.

- **1 Initial.**
 - There is evidence that the enterprise has recognized that the issues exist and need to be addressed. There are, however, no standardized processes; instead there are *ad hoc* approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.



Maturity assessment scale

- **2 Repeatable.**
 - Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.

- **3 Defined.**
 - Procedures have been standardized and documented, and communicated through training. It is, however, left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalization of existing practices



Branswijk
Certifications

Maturity assessment scale

- **4 Managed.**
 - It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
- **5 Optimized.**
 - Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modeling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.



Branswijk
Certifications

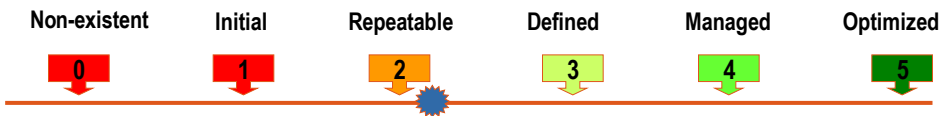
Maturity assessment Questionnaire

Quick Scan Audit Questions IT Security Officer				
Ref.	Questions	Ref.	Score	Expected
A.1 Organizing Information Security				
B.1.1 Organizing Information Security Roles & Responsibilities				
QOIS1	Roles and responsibilities	AOIS1		
QOIS106	Are IT Security Officer information security responsibilities formally assigned, acknowledged and documented within job descriptions?	AOIS106	3	3
QOIS121	Is the XXX IT Security Officer aware of his/her security responsibilities?	AOIS121	3	3
QOIS123	Does the IT Security Officer have unrestricted access to all security relevant information?	AOIS123	3	3
QOIS124	Does the IT Security Officer have unrestricted access to information in other offices?	AOIS124	3	3
B.1.2 Internal Organization				
QC11	Formal Meetings	AC11		
QC1104	Does Belgium IT Security Officer inform ITS Global on changes to the local security organisation?	AC1104	4	4
QC1105	Is there a regular local security team meeting (documentation)?	AC1105	2	4
QC1110	Does the IT Security Officer seek regular support and guidance from ITS Global?	AC1110	4	4



Maturity assessment reports

Maturity Measurement & Reporting



Ranking

Current information security situation at X



- 0 – Security Processes are not applied at all
- 1 – Security Processes are *ad hoc* & disorganized
- 2 – Security Processes follow a regular pattern
- 3 – Security Processes are documented & communicated
- 4 – Security Processes are monitored & measured
- 5 – Security “Best practices” are followed & automated



Maturity assessment reports

Information Security Maturity Score Matrix	A.1 Organizing Information Security	A.2 Asset Classification	A.3 HR Security	A.4 Physical and Environmental Security	A.5 Communications and Operations Management	A.6 Access Control	A.7 Information System Acquisition, Development & Maintenance	A.8 Information Security Incident Management	A.9 Business Continuity Management	A.10 Compliance
Total score	1,84	1,64	1,60	2,48	1,60	1,32	1,55	1,15	1,64	1,17
Expected score	2,48	2,64	2,46	3,00	2,67	1,97	2,68	2,51	3,00	2,13
Overview of Information Security Maturity Score by department										
Network Operations	3,00	-	2,20	2,40	1,75	1,75	2,00	1,43	2,00	1,27
IT Security Officer	1,33	1,00	1,30	1,00	1,50	1,00	-	1,75	1,33	1,00
Helpdesk and Asset Management	2,67	1,94	2,33	1,00	2,00	4,00	-	0,94	2,00	2,00
Application Development	2,00	-	1,00	-	2,00	-	1,01	0,50	1,00	0,70
HR	1,00	-	2,13	-	2,00	-	-	2,00	1,00	2,00
Project Manager	2,00	-	-	-	2,00	-	3,00	1,00	3,00	2,00
Risk Manager & QA	2,50	-	-	-	-	2,50	-	2,33	1,00	2,88
Legal	3,00	-	-	-	3,00	-	-	2,00	-	3,00
Physical Security Officer	3,00	-	2,00	2,82	2,00	3,00	-	1,00	2,50	3,00
CIO & IT Management	2,80	-	-	-	3,00	-	-	1,00	1,00	-



Maturity assessment reports

Network Operations	Current Score	Expected Score
A.1 Organizing Information Security	3	3,00
A.3 HR Security	2,2	3,00
A.4 Physical and Environmental Security	2,4	3,00
A.5 Communications and Operations Management	1,764367816	3,00
A.6 Access Control	1,928571429	3,00
A.7 Information System Acquisition, Development & Maintenance	2	3,00
A.8 Information Security Incident Management	1,428571429	3,00
A.9 Business Continuity Management	2	3,00
A.10 Compliance	1,222727273	3,00



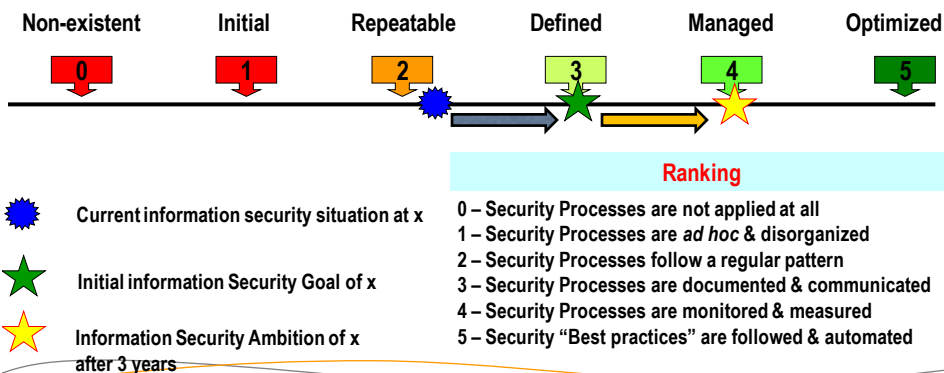
Maturity assessment reports

Physical Security Officer	Current Score	Expected Score
A.1 Organizing Information Security	3	3
A.3 HR Security	2	3,00
A.4 Physical and Environmental Security	2,82	3,00
A.5 Communications and Operations Management	2	3,00
A.6 Access Control	3	3
A.8 Information Security Incident Management	1	3
A.9 Business Continuity Management	2,5	3
A.10 Compliance	3	3

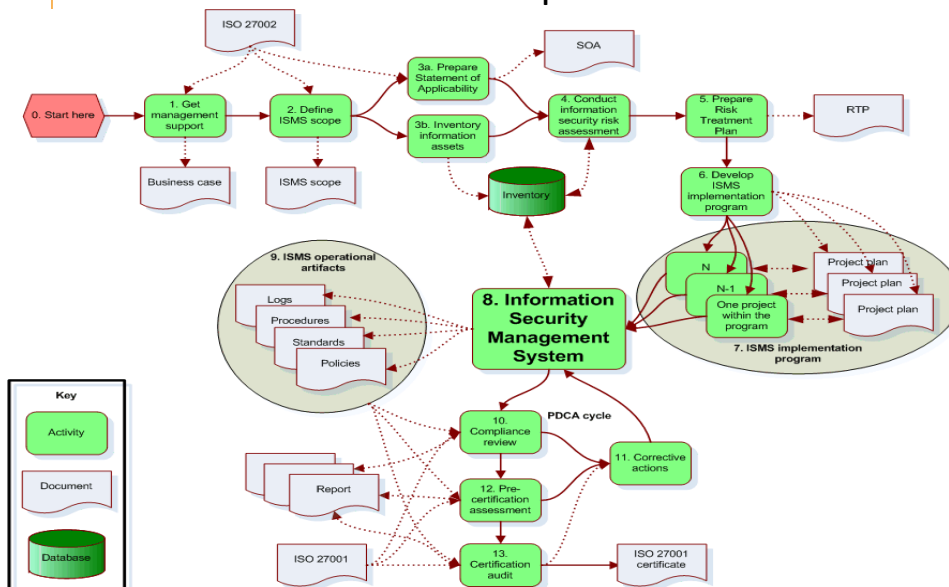


Management view

Maturity Measurement & Reporting



Steps to certification





Step 1 : Get Management approval

- This was for Company x not an issue as the request to go for ISO27001 certification came from management
- Formal Statement Of Commitment was however not in place.
 - One pager signed by CEO



Example paragraph

- As '<Company>'s' Chief Executive Officer, I endorse and support the institution and maintenance of a comprehensive security programme to implement security in all '<Company>'s' present and future activities.





Example paragraph

- To this effect I applaud the initiative and efforts of the 'Security and Risk Management' group to drive forward this corporate wide Information security programme in all its facets, and to enable us, as a company, to obtain accreditation under international standards.



Step 2 : Define ISMS scope

Approach :

- Workshop with management

Outcome :

- Scope defined to be the production plant of the company as it is already certified towards other standards.
 - Start small, think big





Step 3 : Prepare Statement of applicability (SOA)

- Based on previous certifications on the following standards :
 - Ministry of Defense
 - VISA
 - Mastercard
 - ISO 9001



ISO 27001-27002	Min Defense 2003	VISA Security 2002	MasterCard 2004	ISO 9001:2000	Conclusion
4 Information security management system					OK
4.1 General requirements					OK
4 RISK ASSESSMENT AND TREATMENT					OK
4.1 ASSESSING SECURITY RISKS	10		2 - 3 - 4		OK
4.2 TREATING SECURITY RISKS	10		2 - 3 - 4		OK
5 SECURITY POLICY					OK
5.1 INFORMATION SECURITY POLICY	10		4	5	OK
5.1.1 Information security policy document	10		4	5	OK
5.1.2 Review of the information security policy	10		4	5	OK
6 ORGANIZATION OF INFORMATION SECURITY					OK
6.1 INTERNAL ORGANIZATION	1 - 5 - 10		4	5	OK
6.1.1 Management commitment to information security	1 - 5 - 10		4	5	OK
6.1.2 Information security co-ordination	1 - 5 - 10		4	5	OK
6.1.3 Allocation of information security responsibilities	1 - 5 - 10		4	5	OK
6.1.4 Authorization process for information processing facilities	1 - 5 - 10		4	5	OK
6.1.5 Confidentiality agreements	1 - 10		4	6	OK
6.1.6 Contact with authorities	1 - 5 - 10		4	6	OK
6.1.7 Contact with special interest groups	1 - 5 - 10		4	6	OK
6.1.8 Independent review of information security	1 - 5 - 6	1 - 3 - 4 - 5 - 6	4	6	OK
6.2 EXTERNAL PARTIES	1 - 5 - 10	3 - 6	4	6	OK
6.2.1 Identification of risks related to external parties	1 - 5 - 10	3 - 6	4	6	OK
6.2.2 Addressing security when dealing with customers	1 - 5 - 10	3 - 6	4	6	OK
6.2.3 Addressing security in third party agreements	1 - 5 - 10	2 - 3	4	6	OK



SOA

Statement of Applicability

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, CO: contractual obligations, BR/BP: business requirements/adopted best practices, RRA: results of risk assessment, TSE: to some extent

Current as of:
2010 January 20

ISO 27001:2005 Controls			Current Controls	Remarks (Justification for exclusion)	Selected Controls and Reasons for selection				Remarks (Overview of implementation)
Clause	Sec	Control Objective/Control			LR	CO	BR/ BP	RRA	
		5.1 Information Security Policy							
Security Policy	5.1.1	Information Security Policy Document							
	5.1.2	Review of Information Security Policy							
		6.1 Internal Organization							
Organiza- tion of Information security	6.1.1	Management Commitment to information security							
	6.1.2	Information security Co- ordination							
	6.1.3	Allocation of information security Responsibilities							
	6.1.4	Authorization process for Information Processing facilities							
	6.1.5	Confidentiality agreements							
	6.1.6	Contact with authorities							
	6.1.7	Contact with special interest groups							
	6.1.8	Independent review of information security							
		6.2 External Parties							
	6.2.1	Identification of risk related to external parties							
	6.2.2	Addressing security when dealing with customers							
	6.2.3	Addressing security in third party agreements							



Step 4 : Conduct Information Security Risk Management

Approach :

- 2 sessions :
 - One with upper management
 - One with N-1



Selected risks

- Reputation
- Delivery of goods (raw material)
- Access (physical) to building, infrastructure
- Logical access to infrastructure
- Data integrity
- Product integrity
- Resource availability (people, systems, budget, production infrastructure, ...)



Selected risks

- Misconfiguration of systems (accidental, malicious)
- Compliance (regulations, requirements, quality)
- Major disasters (fire, terrorism, ...)
- Major interruptions (power, 3rd party, communication, card distribution, ..)
- Hardware malfunction
- Software malfunction



Questions

3 questions per risk

- What is the impact ..
- What is the probability ..
- What is the level of controls in place ..

Example

What is the impact of a sw malfunction ?

What is the probability of a sw malfunction occurrence ?

What is the level of controls in place to prevent sw malfunction ?



Impact scale

	IMPACT				
	Not Applicable	LOW	MEDIUM	HIGH	CRITICAL
	1	2	3	4	5
Aspect revenu	Aucun	< 10.000 euro	10.000 - 100.000 euro	100.000 - 1.000.000 euro	> 1.000.000 euro
Aspect réglementaire et légal	Aucun	Non respect de règles mineures dans des cas isolés, Minor Admonition	Non respect de règles en quelques occasions, Penalties	Non respect de règles importantes, Major controls	Non respect de règles fondamentales, Governmental intervention
Motivation, formation engagement, rétention	Aucun	Certaines personnes non-clé sont impactées.	certaines groupes (fonctions-activités) sont impactés	Des services / fonctions clé de la société sont impactées de manière importante et durable.	L'entièreté du personnel est impactée de manière importante et durable.
Santé et Protection	Aucun	Risque de blessures, minor injury	Multiple injuries, incapacité de travail Some environmental damage	Serious injury, incapacité long terme, invalidité Serious environmental damage	Risque Mortel, Fatalities, Long lasting environmental damage
Production	Aucun	interruption ponctuelle transparent pour client	interruption affecte > 40% ressources/revenus < 72h interruption affecte < 40% ressources/revenus < 10 jours	interruption affecte > 40% ressources/revenus > 72h toute interruption > 10 jours	production interrompue vers tous les clients > 10 jours
Relation client / Réputation	Aucun	Isolated local event	Extended local event. Short term disruption to confidence	Medium term local event. Medium term disruption to confidence.	Extensive local event; long term disruption to confidence
Efforts spécifiques	Aucun	Impact absorbé dans les activités journalières	Impact spécifique géré par le Middle Management, intervention du Management	Impact significatif géré par le Management, information du Board	Impact énorme demandant l'attention totale du Management et du Board



Probability scale

PROBABILITE					
	Très improbable	Improbable	Probable	très probable	Régulier
	1	2	3	4	5
Temps	Event may occur only in very exceptional circumstances. No occurrences known	Event could occur only in certain circumstances.	Event could occur at some time.	Event will probably occur at some time.	Event will probably occur in most circumstances.
	Komt maximaal elke 30 jaar voor	Komt maximaal elke 5 jaar voor	Komt maximaal elke jaar voor	Komt maximaal elke maand voor	Komt op dagelijks/wekelijks basis voor

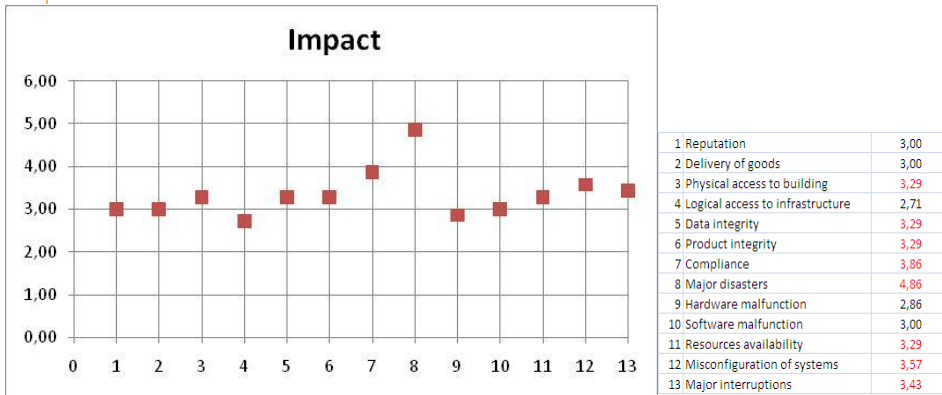


Control level scale

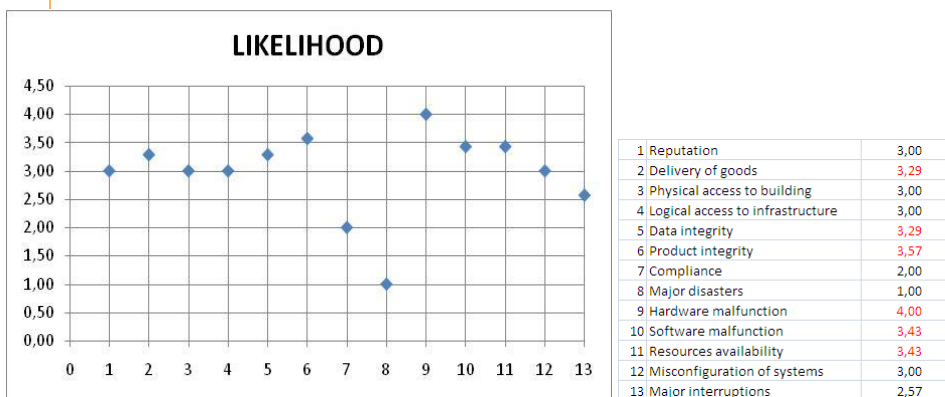
MESURES DE CONTROLE					
	Très faible	Faible	Moyen	Elevé	Optimal
	1	2	3	4	5
Degré de maturité : sommaire	Initialisé / Ad hoc	Non-formalisé / Répétition	Systématique / Défini	Intégré / Mesuré	Optimisé
Degré de maturité : explication	prise de conscience du risque et projet de contrôle interne	contrôle interne sans procédure et non connu de tous	procédure exhaustive et formations au contrôle interne	suivi et amélioration du contrôle interne récurrent	suivi et mise à jour du contrôle interne en temps réel
	Uitvoering van controle is zeer sterk afhankelijk van het individu	Groep voert dezelfde controles uit op basis van ervaring	Gedocumenteerde en gestandaardiseerde controles met opleiding	monitoring en meting van uitgevoerde controles met aanpassing waar nodig	solide controles op basis van continue verbeteringen en benchmarking met gebruik van tools



Measure the impact



Measure the likelihood





Measure the risk

Threat	Probability	Impact	Risk
Reputation	3,00	3,00	3,00
Delivery of goods	3,29	3,00	3,14
Physical access to building	3,00	3,29	3,14
Logical access to infrastructure	3,00	2,71	2,86
Data integrity	3,29	3,29	3,29
Product integrity	3,57	3,29	3,43
Compliance	2,00	3,86	2,93
Major disasters	1,00	4,86	2,93
Hardware malfunction	4,00	2,86	3,43
Software malfunction	3,43	3,00	3,21
Resources availability	3,43	3,29	3,36
Misconfiguration of systems	3,00	3,57	3,29
Major interruptions	2,57	3,43	3,00

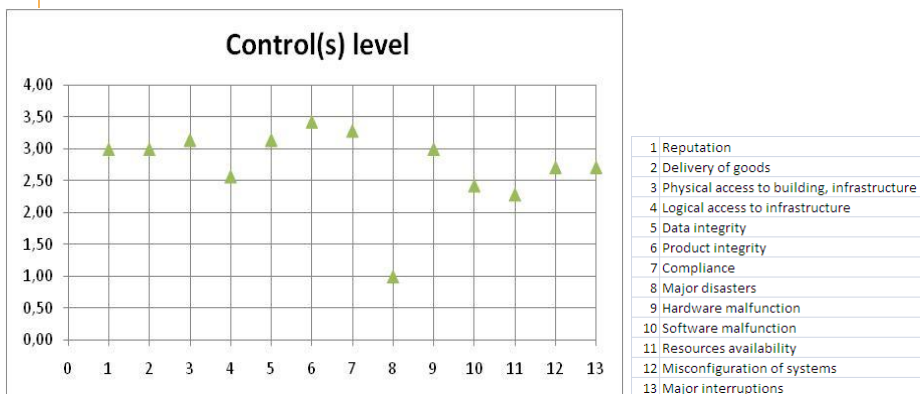


Measure the risk

High risk	High impact	High likelihood
Data integrity	Physical access	Delivery of goods
Product integrity	Compliance	Hardware malfunction
Resources availability	Major disaster	Software Malfunction
	Major interruptions	
	Misconfiguration of the systems	



Measure the controls



Risks vs Controls

Threat	Control(s) level	Risk	Residual
Reputation	3,00	3,00	0,00
Delivery of goods	3,00	3,14	0,14
Physical access to building	3,14	3,14	0,00
Logical access to infrastructure	2,57	2,86	0,29
Data integrity	3,14	3,29	0,14
Product integrity	3,43	3,43	0,00
Compliance	3,29	2,93	-0,36
Major disasters	1,00	2,93	1,93
Hardware malfunction	3,00	3,43	0,43
Software malfunction	2,43	3,21	0,79
Resources availability	2,29	3,36	1,07
Misconfiguration of systems	2,71	3,29	0,57
Major interruptions	2,71	3,00	0,29



Risks vs Controls

VERY HIGH RESIDUAL	HIGH RESIDUAL	CONTROLLED
Major Disasters	Hardware malfunction	Reputation
Ressources availability	Major interruptions	Physical access to the building
Software malfunction	Logical access to infrastructure	Product integrity
Misconfigurations of the systems	Delivery of goods	Compliance
	Data integrity	



Risks assesment - summary

Threat	Probability	Impact	Control(s) level	Risk	Residual
Reputation	3,00	3,00	3,00	3,00	0,00
Delivery of goods	3,29	3,00	3,00	3,14	0,14
Physical access to building	3,00	3,29	3,14	3,14	0,00
Logical access to infrastructure	3,00	2,71	2,57	2,86	0,29
Data integrity	3,29	3,29	3,14	3,29	0,14
Product integrity	3,57	3,29	3,43	3,43	0,00
Compliance	2,00	3,86	3,29	2,93	-0,36
Major disasters	1,00	4,86	1,00	2,93	1,93
Hardware malfunction	4,00	2,86	3,00	3,43	0,43
Software malfunction	3,43	3,00	2,43	3,21	0,79
Resources availability	3,43	3,29	2,29	3,36	1,07
Misconfiguration of systems	3,00	3,57	2,71	3,29	0,57
Major interruptions	2,57	3,43	2,71	3,00	0,29



Step 5 : Prepare Risk Treatment Plan (RTP)

- Risk is a feature of business life and since it is impractical and uneconomical to eliminate all risks, every organization has a level of risk it will accept. Faced with risk, organizations have four strategic choices:
 - Terminate the activity giving rise to risk (**Terminate**)
 - Transfer risk to another party (**Transfer**)
 - Reduce risk by using of appropriate control measures or mechanisms (**Treat**)
 - Accept the risk (**Tolerate**)



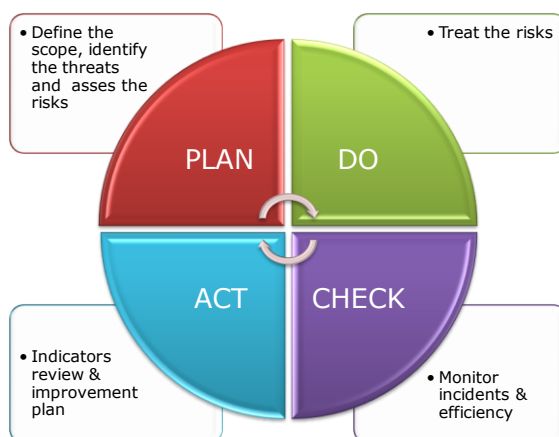
Step 5 : Prepare Risk Treatment Plan (RTP)

- Management takes the decision on what to do with the risk
- Risk manager can propose actions

(VERY) HIGH RESIDUAL RISKS	RISK TREATMENT PROPOSAL	OWNER
Major Disasters	Treat - BCP framework for ID documents	SCO
Ressources availability	Treat SpoF : competences & equipment	AKO
Software malfunction	Treat – apply change control management IT applications deployments	XDL - JMJ
Misconfigurations of the systems	Treat – control access to production equipment configurations and document the configurations on KERN & CML-CMI	XDL - PDE
Hardware malfunction	Treat – increase preventive maintenance on production equipment	PDE
Major interruptions	Tolerate	
Logical access to infrastructure	Tolerate	
Delivery of goods	Treat – intervention at card manufacturer to ensure stability in card body properties for laser engraving	JMJ-SCO
Data integrity	Treat - Reinforce QC personalization according to new identified risks	SCO



... On regular base





Step 6 and 7: ISMS implementation plan

- Management took the decision to integrate the ISMS in their existing Quality Management System (QMS)
- Programs are initiated to :
 - integrate Information Security Management in the QMS
 - Proper document Information Security based on the ISO 27002 standard
 - Set-up the security organization



Step 6 and 7: ISMS implementation plan





Step 8 and 9: Manage and document ISMS

- Information security will be integrated in the already operational QMS system.
- Management of QMS(ISMS) is described in Quality manual
- Procedures and guiding documents need some additional statements with regards to Information Security related topics

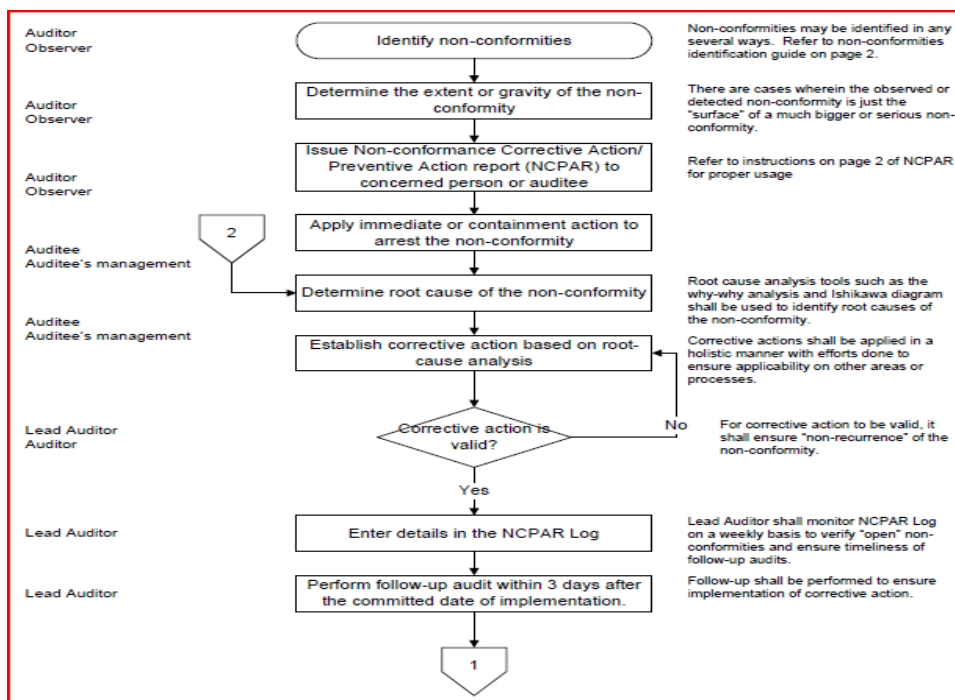


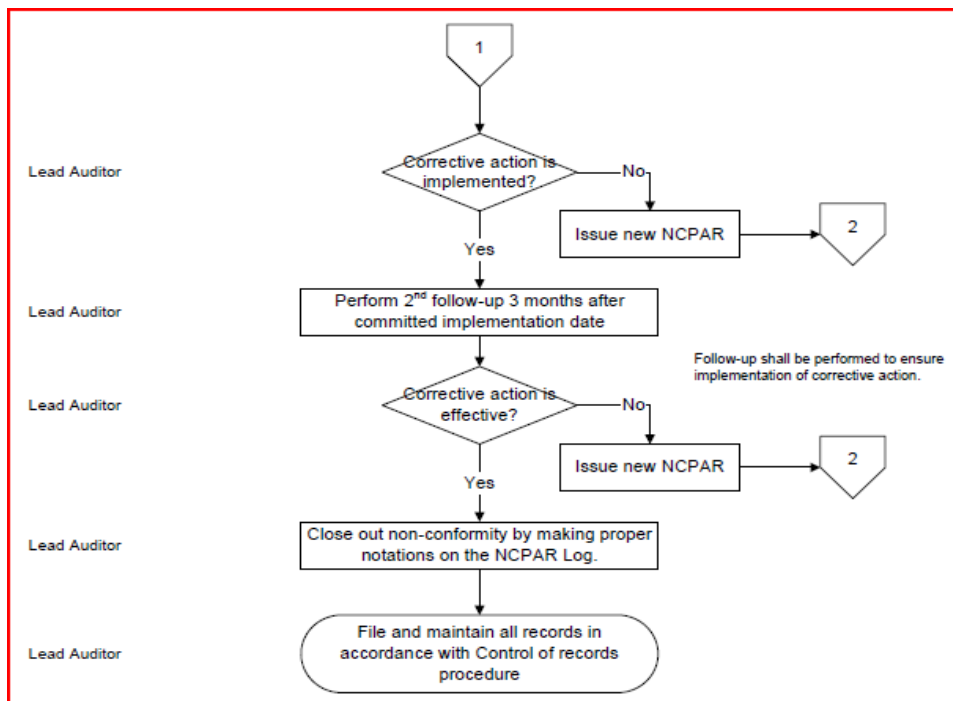
Step 10 : Compliance Review

ISM audit test	Findings
<p>12.5 Security in development and support processes. Review change control procedures. Are they documented and appropriate? Do they cover significant changes to computing and telecommunications equipment (hardware), key operating system parameters and software, application software etc.? Review a small sample of change control records. Are changes properly documented, justified and authorized by management?</p>	
<p>12.6 Technical vulnerability management. Evaluate how the organization identifies and responds to technical vulnerabilities in desktops, servers, applications, network devices and other components, for example by reviewing change control records for evidence relating to recent patches. Are there suitable processes in place to review the inventory of systems and identify whether announced vulnerabilities are relevant? Are patches assessed for applicability and risks before being implemented? Are the processes for implementing urgent patches sufficiently slick and comprehensive? To what extent does the organization depend on automated patch management, in effect accepting the associated risks of implementing rogue patches? Look for any evidence of important systems that have not been maintained at current release levels and/or patched against known vulnerabilities.</p>	
<p>13. Information security incident management</p>	
<p>13.1 Reporting information security events and weaknesses. Check the processes for reporting security events and weaknesses. Trace the process using a sample of documentation such as Help Desk records, comparing what actually happened with the policies, procedures and guidelines. Confirm that those who should be reporting security events and weaknesses are aware of, and in fact use, the process.</p>	



Step 11 : Corrective actions





Step 12 : Pre-certification assessment

- Partially done in Step 10 : Compliance review
- Documentation review (Internal and auditor)
 - Are the Mandatory documents in place ?



Mandatory documents

Management commitment to implement ISMS
ISMS scope
ISMS policy
ISMS implementation plan
ISMS operating procedures
ISMS recording & control of documents
Information assets inventory
Risk assessment methodology
Risk assessment report
Risk relations & selection of controls
Risk treatment plan & selection of controls
Statement Of Applicability



Mandatory documents

Management approval for implementing ISMS
Corporate Security policy
Detailed security policies
Information security procedure
Information security metrics
Document control procedure
Records control procedure (QMS)
Security awareness, training and education records
Internal ISMS audit plans & procedures (QMS)
Corrective action procedure
Preventive action procedures
Management review plans & reports



Step 13 : Certification audit

- Document review by Certification Body
- Implementation review by Certification Body
- Evaluation of all information by Certification Body
- Certification decision by Certification Body



Step 13 : Certification audit

Categories of issues in a Certification Audit

- MAJOR issue found : Action item
 - Audit stopped immediately
 - Company needs to resolve major issue before audit can be restarted (unlimited timeframe)
- SIGNIFICANT issue found : Action item
 - Audit continues
 - Company gets specific timeframe to resolve significant issue
 - Auditor (Certification Body) reviews at the end of the certification audit if significant issue is resolved based on the actions taken by Company



Step 13 : Certification audit

Categories of issues in a Certification Audit

- MINOR issue found : To be planned
 - Audit continues
 - Minor issue is listed in a special annex and will receive special attention during the first ISO 27001 control audit (Certification Body)



Step 13 : Certification audit

- Findings will be recorded in **N**on-conformance **C**orrective /**P**reventive **A**ction **R**eport (**NCPAR**) log





Example NCPAR log

NCPAR No. NC- xy-000	Non-conformity/Corrective & Preventive Action Report (NCPAR)	Date NC Found:
Department or Section where NC is found:		
1. DETAILS: Nonconformity raised as a result of:		
<input type="checkbox"/> Internal audit	<input type="checkbox"/> Customer complaint	<input type="checkbox"/> IS Incident, indicate IS number _____
<input type="checkbox"/> Process non-conformity	<input type="checkbox"/> Suggestion (improvement) _____	
<input type="checkbox"/> Product non-conformity	<input type="checkbox"/> Others _____	
2. REFERENCES: Documents used or referred to: (e.g. manuals, procedures, flowcharts, standards, records, documents, etc.)		
3. NON-CONFORMITY: Description of nonconformity, suggestion, complaint or incident.		
Detected or Observed by:	Department:	
4. DISPOSITION: Immediate remedial action		
Proposed by:	Date:	Implementation date:
5. INVESTIGATION: Cause of nonconformity: (investigation shall be conducted by the department or section where the nonconformity was found)		
Investigated by:	Date investigation started:	
	Date investigation finished:	

6. CORRECTIVE/PREVENTIVE ACTION: (Preventive action is only required for <u>potential non-conformities</u>). Fill ONLY EITHER "Corrective Action" OR "Preventive Action"			
Corrective Action:		Preventive Action:	
Proposed by:		Date:	
		Proposed implementation date:	
7. VERIFICATION OF VALIDITY OF CORRECTIVE "or" PREVENTIVE ACTION:			
<input type="checkbox"/> Addresses the root cause? <input type="checkbox"/> Prevents recurrence? <input type="checkbox"/> Valid <input type="checkbox"/> Invalid. Issue new NCPAR		<input type="checkbox"/> Addresses the root cause? <input type="checkbox"/> Prevents occurrence? <input type="checkbox"/> Valid <input type="checkbox"/> Invalid. Issue new NCPAR	
Remarks: _____		Remarks: _____	
Signature:	Date:	Signature:	Date:
(Lead Auditor)		(Lead Auditor)	
8. FOLLOW-UP OF IMPLEMENTATION CORRECTIVE/PREVENTIVE ACTION TAKEN:			
Implementation of corrective action is: <input type="checkbox"/> Implemented <input type="checkbox"/> Not implemented. Issue new NCPAR		Implementation of preventive action is: <input type="checkbox"/> Implemented <input type="checkbox"/> Not implemented. Issue new NCPAR	
Remarks: _____		Remarks: _____	
Signature:	Date:	Signature:	Date:
(Lead Auditor)		(Lead Auditor)	



9. VERIFICATION OF EFFECTIVENESS OF IMPLEMENTED CORRECTIVE/PREVENTIVE ACTION:			
Corrective action is: <input type="checkbox"/> Effective <input type="checkbox"/> Not effective. Issue new NCPAR		Preventive Action: <input type="checkbox"/> Effective <input type="checkbox"/> Not effective. Issue new NCPAR	
Remarks: _____		Remarks: _____	
Signature:		Signature:	
(Lead Auditor)		(Lead Auditor)	
Date:		Date:	



