Global Information Assurance Certification Paper

Development of an ISMS for a Storage Area Network

G7799

Practical Assignment

Version 1.1

20th of September 2004

Stéphane Grundschober
Track 11c – Orlando
2-7 April 2004

Table of Contents

List of Figures

1 Abstract

This document presents the development steps followed to design, implement, review and maintain an Information Security Management System (ISMS). It follows the ISO17799 standard.

The structure of this present document follows the standard's concept of "Plan, Do, Check & Act".

In parts one and two, "Plan", we define the scope of the ISMS, in our case a Storage Area Network (SAN). We describe the existing security culture and organisation, and how the ISMS will have to fit in this organisation. We extensively review the actual security management, in order to identify missing elements that will be implemented by the ISMS

In part three, "Do", for three elements of the ISMS selected in part two, we detail the actual implementation steps.

In part four, "Check", we design audit checklists for the same three elements. These checklists allow external auditors to verify the correct implementation of the ISMS, as well as to ensure all key personals are actually aware of the processes.

In the last part, "Act", we define the processes needed to ensure a constant maintenance of the ISMS. By collecting the output of reviews, audits, security incidents or insight from operational activities, we can update the ISMS and complement its implementation.

This document does not have the pretension of being an exhaustive ISMS for Storage Area Networks. It shows nonetheless the process needed to implement a full ISMS for the considered system, along with practical examples from a real system.

In parallel to the writing of this document, the whole ISMS is actually developed for the organisation.

2 Document Conventions

When you read this practical assignment, you will see that certain words are represented in different fonts and typefaces. The types of words that are represented this way include the following:

URL	Web URL's are shown in this style.
[1]	A pointer to a reference listed in section 8

3 Part One: Define the system

This chapter describes the system chosen for implementing an ISMS following ISO17799. We then describe the organisation and its security culture. Finally, we define the scope of the ISMS.

3.1 System selection for ISMS implementation

The goal of this work is to implement an ISMS for our Dell Storage Area Network (SAN) system.

This SAN is used by various **internal** servers, fulfilling a variety of services:

- "Home" drive for users
- File server
- MS Sharepoint [1] server
- Intranet web server
- SQL server (mostly used by sharepoint)
- Management server for the SAN itself

These servers host files that are essential for the daily business of our organisation. The files have various security classifications, going up to "confidential".

The rack servers are connected via two High Availability Fibre Channel switches to the storage array. A Tape Library is also connected via Fibre Channel to the switches for backup purposes.

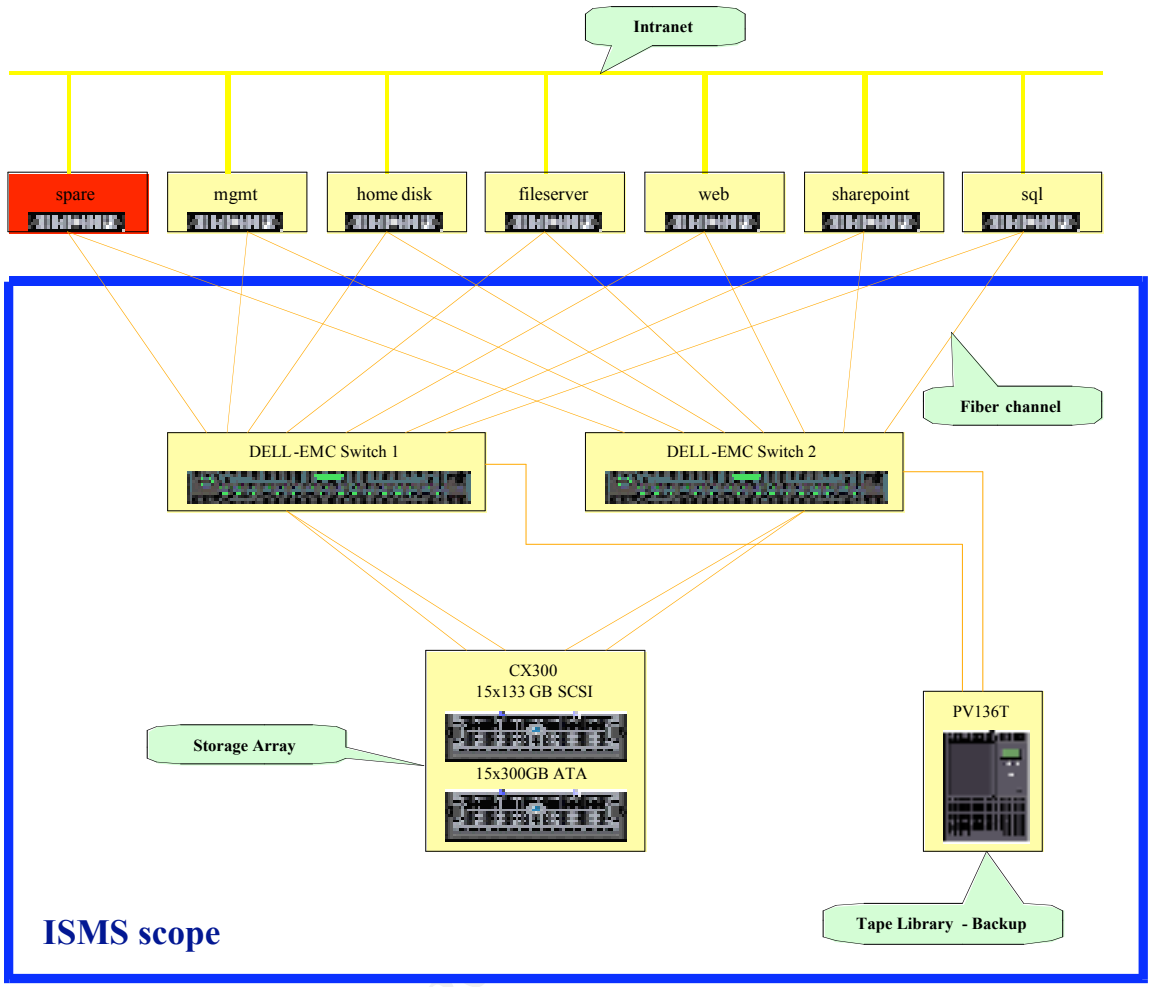


Figure 1: SAN architecture[1]

3.2 Organisation description

The SAN belongs to the Research and Development group. This group consists of about 180 employees, all located in the same building.
The group has its own authority on the IT systems and networks. It uses some resources from the parent company (like domain authentication, email platform, etc…).
The parent company is structured in a holding, each group companies having their own authority.

3.3 Existing security organisation

The holding Head Quarters (HQ) issued general security policy documents. These documents define:

- General security goals: Vision, Mission, protection of persons, immaterial goods, material goods and services

[1] graphic taken with permission from the SAN manager

- Requirements for the protection of information against integrity, confidentiality and availability breaches (formulated in a very generic manner)
- Proper use of IT and Communication means
- Security organisation in the group companies
- Company wide security forum for coordination
- Development of an ISMS that is standardized and must be "auditable". Each group company is then free to choose whichever ISMS standard they want.

Our R&D group has then developed the following security elements:

- Attribution of the role of security manager (representing the group at the security forum)
- Attribution of the role of IT security manager (responsible for the actual implementation and management of IT security controls)
- Building of a "security team", i.e. employees working in the field of security R&D, in order to support the IT security manager in operational activities
- Security directive (provide details of the holding's policy requirements)
- Guidelines
- Manuals (how to install anti-virus, how to configure Windows automatic update, …)
- Security Awareness Training

This security management does not follow an ISMS standard. It has up to now been built following best practice, employees' experience, or after security incidents revealed weaknesses in the security management.

The SAN itself has no proper ISMS. Documentation about the installed systems and key configuration is available and maintained in collaboration with Dell, in order to obtain Gold Support.
After a first interview with the SAN manager, it appears that many good security principles are applied, but not actually documented (informal processes).

3.4 Scope of the ISMS

Recognising the need to adapt our security organisation to a known standard, especially after the HQ requirement for a known and auditable ISMS, it has been decided to evaluate our fitness to the ISO17799 standard, and the resources needed to obtain compliance with the standard.

In order to perform this evaluation, it has been decided **to implement an ISMS specific to our SAN**, in order to gain experience with such an implementation. **This doesn't include the servers using the SAN.**

Expected results are:

- Identification of existing/missing standard controls, as described in our policy/directive/guidelines
- Implementation of the ISMS, focusing on the SAN only
- Evaluation of the resources needed to implement the ISMS for the SAN only (with the ultimate goal of being able to extrapolate for the whole organisation)

Any missing element from the standard, and applicable to the SAN, will be developed and documented. It will be therefore part of the existing security documentation (policy/directive/guidelines). It is not planned to change the existing documents, but to complement them.

4 Part Two: Plan

4.1 Projects steps

Once the goals of the project have been accepted by the organisation's management (Chief Information Officer and IT Security Manager), we could start the project.

A review team has been formed, consisting of:

- CIO
- IT Security manager
- In House Security specialists (security team)

Due to the limited budget and scope, and also because this project is used to obtain the G7799 certification, only one employee (i.e. the author of this document) is actually performing the whole evaluation and implementation.

The project steps have been defined as:

- Review of existing security policies/directives
- Mapping of existing security policies/directives on the ISO17799 standard
- Identification of missing elements and applicability
- Development of the ISMS
- Request the implementation of ISMS (and corresponding budget)

4.1.1 Documentation framework

In order to support the mapping of existing security policies/directives on the standard and the following identification of missing elements, we developed a framework based on Sharepoint and Infopath (both from Microsoft).

It consists in a collection of forms (xml data rendered in Infopath), containing the following fields:

- Paragraph number of the standard
- Audit question (taken from SANS' SCORE checklist project [2])
- Findings
- Findings date
- If the item is specific for the organisation
- If the item is specific for the system
- Link to intranet documents (if available)

- If the item is applicable
- A subjective compliance level (between 0 and 1)
- An objective compliance status (yes or no)
- Priority level of the item (i.e. in case on non-compliance, is it important to solve this item first?)
- An optional “notes” field
- An optional (non-)applicability statement
- Extract of the standard itself as reference

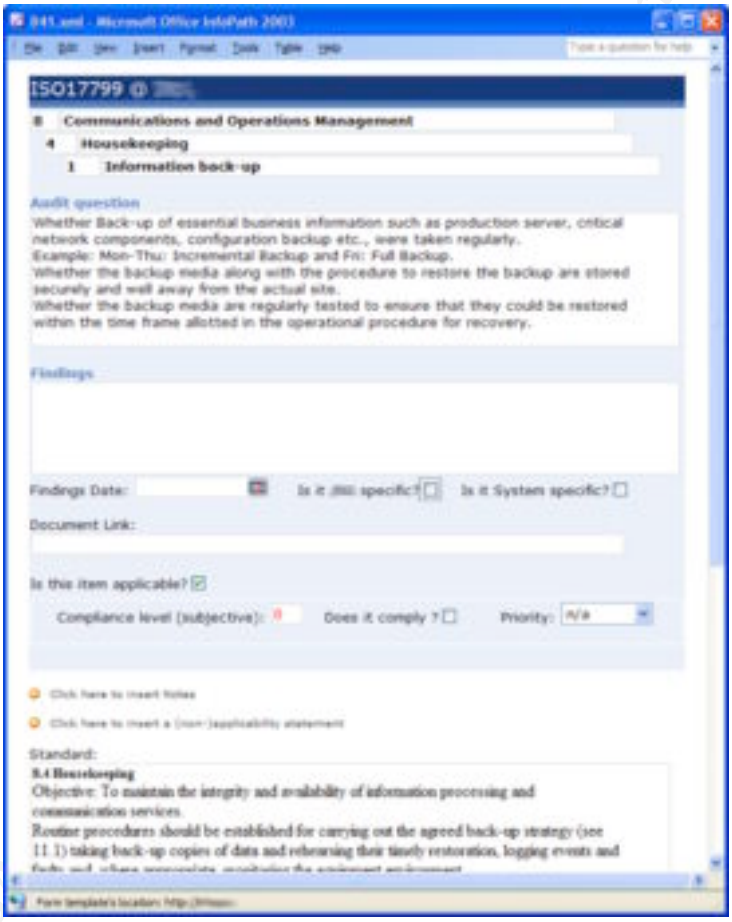


Figure 2: Empty form for one item of the standard

Once completed and stored in a “form library” on a sharepoint site, it is possible to export some fields and create “views”:

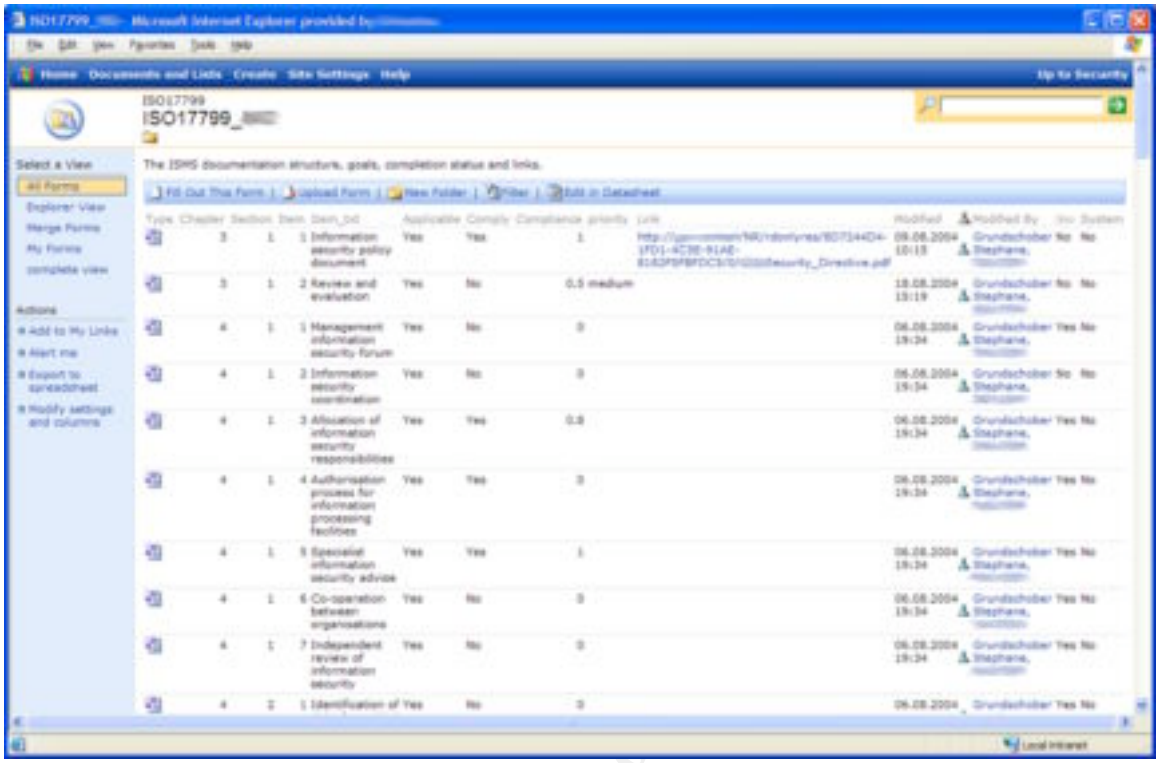


Figure 3: Sharepoint form library

This system allows an easy tracking of the ISMS documentation and can be potentially exported to databases or other custom reporting tools.

4.2 ISMS management structure

This ISMS has to be integrated in the existing security management structure. As we are a relatively small group, the existing organisation (see Figure 4) is sufficient for fulfilling ISMS management requirements.

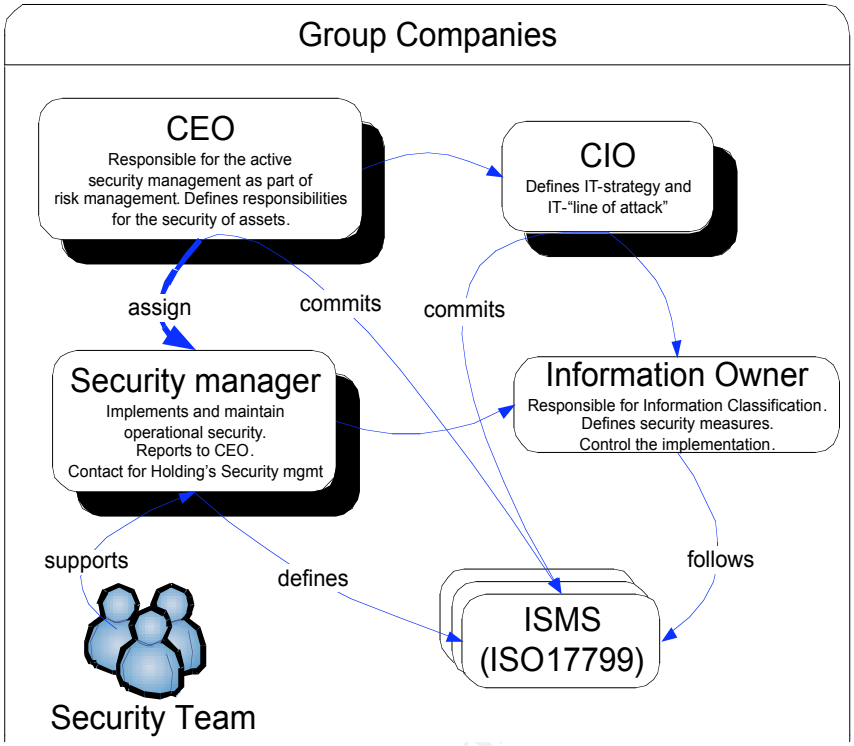


Figure 4: Security management organisation

The following list describes the security management relevant functions of the various roles defined in the security organisation:

- CEO: he/she is responsible for the active security management, as part of risk management. He/she defines responsibilities. He/she assigns the security manager and the CIO. He/she commits to a standardised and auditable ISMS.
- CIO: he/she defines the "line of attack", i.e. the resources to be invested in security management, and by consequence, how far the security should be implemented.
- Security Manager: he/she leads the security activities. He/she is responsible for the implementation and maintenance of operational security.
- Security Team: a group of security experts picked among the group employees. Its goal is to support the security manager in all aspects of both security management and operational security. This team consists as of today of 8 people, bringing competences in the domain of policies writing, ISO17799, firewall, VPN, general network management and security, OS Hardening, IDS, Wireless LAN security, virus protection, cryptography, security training.

- Information Owner: any person producing and managing information. This is basically any employee of the group. He/she is responsible for the correct classification of its information, and its proper management.

4.3 Identification of missing/incomplete policies

With the help of the documentation framework (as described in section 4.1.1), we reviewed all existing policies and processes (including informal ones). For each item of the standard, we checked if it was applicable to the scope of our ISMS (the SAN only), if it was specific for the system (or if on the other hand it was more a requirement for the organisation as a whole).

For each applicable item, we gave an objective compliance result (yes or no). In addition, we tried to give a subjective compliance level (between 0 and 1), in order to capture the existence of informal processes. For example, an informal process which is well lived and strictly followed but not documented receives a score 0.8, i.e. non-compliant (needs to be formalised), but is already well done. Following this compliance judgement, we also gave a resolution priority (low-medium-high) in order to facilitate the prioritisation of the following work.

This is a summary of this review work:

ISO 17799 Chapters	Applicable	System specific	Compliance	
			Count	average
3. Security Policy	2 of 2	0 of 2	1 of 2	0.9
4. Organisational Security	8 of 10	3 of 8	6 of 8	0.7
5. Asset classification and control	3 of 3	1 of 3	3 of 3	0.8
6. Personnel security	10 of 10	5 of 10	7 of 10	0.8
7. Physical and Environmental Security	9 of 13	9 of 9	6 of 9	0.7
8. Communications and Operations Management	13 of 24	12 of 13	9 of 13	0.7
9. Access Control	16 of 31	13 of 16	11 of 16	0.7
10. System development and maintenance	6 of 18	5 of 6	3 of 6	0.5
11. Business Continuity Management	5 of 5	5 of 5	0 of 5	0
12. Compliance	7 of 11	7 of 7	0 of 7	0

Among the various missing policies and processes, we will describe in the following paragraphs only three new policies. This should be enough to demonstrate the procedure followed, without killing the reader with pages of boring policies! Of course, we have planned the implementation of all missing policies.

4.3.1 Policies chosen for implementation

Policy Name: Secure disposal of Media

Purpose: Ensure that Media, especially backup tapes, are securely disposed once they have reached the end of their lifetime. As they contain sensitive information, they must be appropriately destroyed to ensure no information leak can occur.

Audience: the Backup Managers

Area of standard addressed: Section 8.6.2 Communications and Operations Management, Media handling and Security, Disposal of Media

Policy Name: Business continuity management

Purpose: "To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters." [3]

Audience: the SAN managers

Area of the standard addressed: Chapter 11 Business Continuity Management

Policy Name: Collection of evidence in case of suspected policy or law breach

Purpose: Define formal procedure to follow in order to secure data on the SAN in case of suspected breach of internal policy, or in case of violation of laws. The procedure must maintain a proper trail of evidence which can be accepted in a legal procedure.

Audience: SAN/Backup manager, Security Officer

Area of the standard addressed: Section 12.1.7 Compliance, Compliance with legal requirements, Collection of evidence

4.4 Main risks

Ideally, we should perform a system wide risk assessment, following a method such as FEMCA[2], in order to identify all risks against the functional objectives of our SAN system (i.e. provide storage to critical servers, with a high availability of 99.5%, and effective daily backups with a defined restore capability, …)

In order to keep this document short and consistent with the previous sections, we will only perform a "fishbone"[3] cause and effect analysis tailored to the topics addressed by the three policies chosen in section 4.3.1.

4.4.1 Risk analysis for "Secure disposal of media"

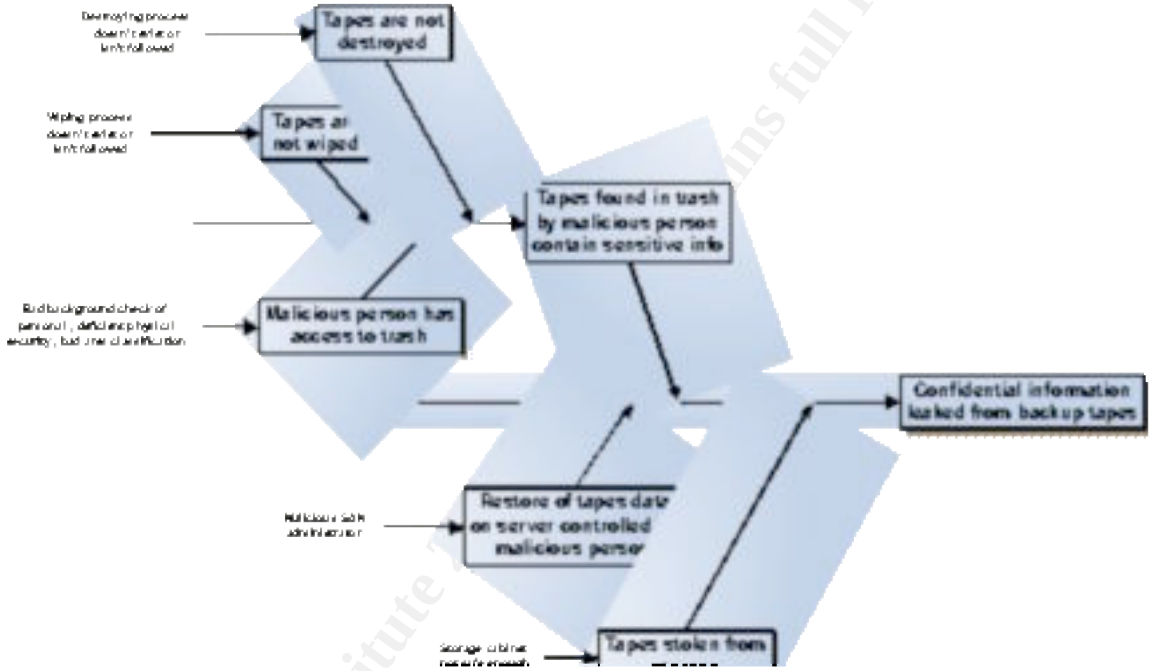


Figure 5: Fishbone diagram "secure disposal of media"

Nature of the threat: Malicious Information disclosure/theft

Cause	Vulnerability	
Tapes stolen from storage	Storage cabinet not safe enough	
Likelihood	**Impact**	**Risk level**
Medium (currently only a locked cabinet)	High	High

[2] Additional information about FMECA: http://www.fmeca.com/ffmethod/history.htm
[3] Description of the Fishbone cause and effect analysis method: http://www.skymark.com/resources/tools/cause.asp

Cause	Vulnerability		
Restore of tapes data on server controlled by malicious person	Malicious SAN or server administrator		
Likelihood		**Impact**	**Risk level**
Low		High	Low-Medium

Cause	Vulnerability		
Tapes found in trash by malicious person contain sensitive info	- Trash is not labeled as “confidential” - Tapes are not wiped - Tapes are not destroyed		
Likelihood		**Impact**	**Risk level**
High (no documented process)		High	High

Description of the control selected: We will implement a wiping process for tapes which have reached their end of life. We will also use a safe instead of a simple locked cabinet to store the tapes.

Reason for selecting control: With these two controls we cover the two identified high risks. Moreover, they are easy to implement.

Risk level after implementing control: The risk level falls down to low for the two high risks, as the whole corresponding branches of the fishbone diagram disappear.

4.4.2 Risk analysis for "Business continuity management"

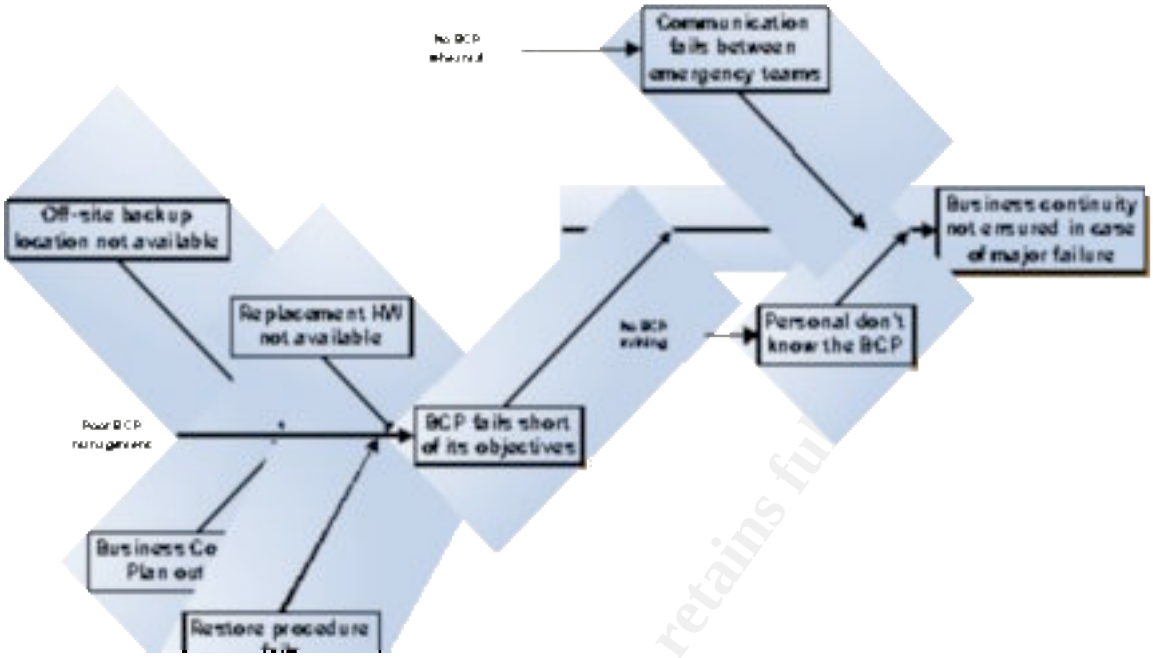


Figure 6: Fishbone diagram "Business Continuity Management"

Nature of threat: Environmental, Deliberate and Accidental threats impacting the business functions of the SAN, leading to an interruption of business continuity

Cause	Vulnerability	
Personal don't know the Business Continuity Plan (BCP)	No training of personal	
Likelihood	**Impact**	**Risk level**
High (currently no BCP)	High	High

Cause	Vulnerability	
Communication fails between emergency teams	No rehearsal/testing of BCP	
Likelihood	**Impact**	**Risk level**
High (currently no BCP)	High	High

Cause	Vulnerability	
BCP fails short of its objectives	No proper management of BCP	
Likelihood	**Impact**	**Risk level**
High (currently no BCP)	High	High

Description of the control selected: We will initiate a proper BCP management, including regular review and rehearsal.

Reason for selecting control: As the whole BCP management process is actually missing, this is a first step.

Risk level after implementing control: We hope to be able to reduce the risk level to low, but this may take time. Further risk assessments, going into more details of the implementation of the BCP, will have to confirm the successful implementation.

4.4.3 Risk analysis of "Collection of evidence in case of suspected policy or law breach"

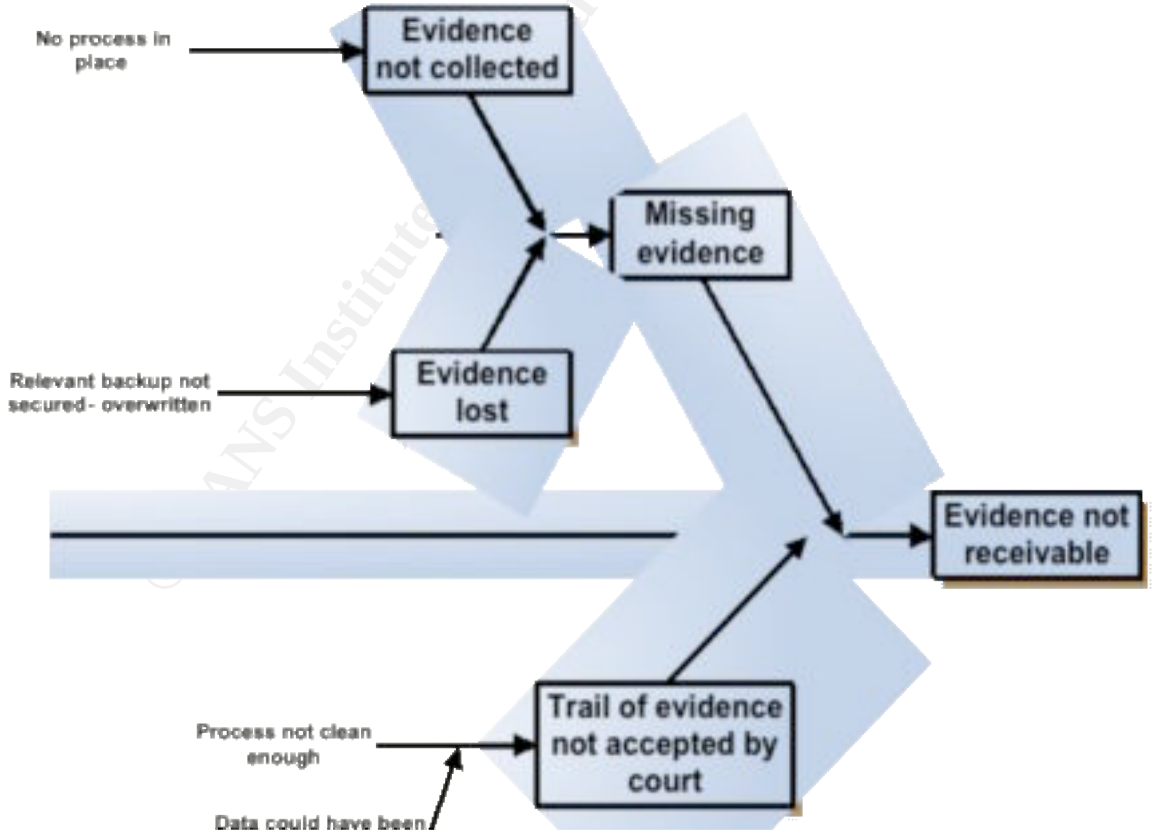


Figure 7: Fisbone diagram "Collection of evidence in case of suspected policy or law breach"

Nature of threat: Accidental loss of evidence, or loss of integrity of evidence trail due to negligence

Cause	Vulnerability	
Missing evidence	No process in place detailing what to do and when to secure data on the SAN in case of suspicion of policy breach or law breach.	
Likelihood	**Impact**	**Risk level**
High (currently no process)	Medium[4]	Medium

Cause	Vulnerability	
Trail of evidence not accepted by court	Process doesn't follow best practice in order to maintain the integrity of the evidence trail and to show due care in its handling.	
Likelihood	**Impact**	**Risk level**
High (currently no process)	Medium	Medium

Description of the control selected: We will initiate the development of a proper evidence collection and maintenance process. It will include initiation by Human Ressource, and will be run under the supervision of the Security Officer. Advice from legal and data privacy experts will be sought.

Reason for selecting control: As the whole process is actually missing, this is a first step.

Risk level after implementing control: Once the process is implemented and tested, we should reach a "low" risk level, as evidence will be collected and managed following best practice.

[4] We classified the Impact as medium, as it is not an immediate threat to the business objectives of the SAN (i.e. provide storage)

5 Part Three: Do

Using the three elements identified in Part Two, we will describe the steps to be taken to implement the improvements.

5.1 Secure disposal of media

Problem: There is no documented process about secure disposal of backup tapes, once they have reached their end of life. This can lead to a potential disclosure of confidential information, if a malicious person manages to find such a discarded tape.

Action: Develop a procedure for secure disposal of media

Steps:

- Define under which conditions a tape is deemed to be at “end of life” (number of seeks, number of soft errors, age, maximum legal storage time, …). Find references, like [4]
- Design a wiping method (either supported by the tape library, or physically with a degausser for example)
- Store off-site tapes in a safe instead of a closed cabinet. Define specifications for the environment inside the safe (hygrometry, temperature) and implement an autonomous regulation system. This is needed in order to have confidence in the “shelf life-time” of the tapes, and not be subject to accelerated aging.
- Document the procedure for identifying “end of life” tapes and for wiping it. Document auditing procedures.
- Obtain management sign-off of the documents

5.2 Business continuity management

Problem: No business continuity management process is in place. This lead to various consequences:

- No committed business continuity strategy: the SAN managers are left alone without management directions. They have designed the SAN and backup systems to their best. It has never been confronted to the actual business objectives of the SAN. The developed system can therefore be either under-developed as well as over developed. Resources for the proper management of the system, and its backup system (including support and maintenance) must be taken from the general operation budget of the group. This can lead, especially in case of wrong management prioritization, to the hijacking of budget for other non-critical systems.

- Failure of existing informal business continuity/recovery plans: because BCP/BRP plans do not exist, it is extremely difficult to say if the existing backup measures will be actually appropriate in case of failure of the system (from either accidental causes as well as environmental and malicious causes). Recovery procedures have never been trained.

Action: Develop a Business Continuity Plan, including review and rehearsal.

Steps:

- Obtain management buy-in (and resources) for the development of a BCP
- Define precisely the business objectives (or functions) of the SAN
- Develop adequate Business Continuity measures to ensure adequate operation of the SAN in case of a major failure (this would include the definition of various operation levels, depending on the criticality of the function)
- Obtain management sign-off of the BCP and accompanying measures.
- Review existing and planned measures against the business functions of the SAN. Schedule this review at least once a year.
- Setup a testing procedure (BCP rehearsal) simulating a major failure. Perform and schedule this simulation at least once a year.

5.3 Collection of evidence in case of suspected policy or law breach

Problem: There is currently no process defining under which conditions and how data should be collected in order to support a disciplinary or legal procedure. This can lead to variable treatments from case to case (even to undue influence of the SAN manager to keep/destroy evidence), to a loss of integrity of the trail of evidence, or even to the loss of evidence.

Action: Develop procedures for proper collection of evidence in case of suspected policy or law breach.

Steps:

- Seek advice from Human Ressource and Legal, about their requirements in evidence collection
- Obtain statement from Data Privacy champion, more specifically how long such information can be stored
- Develop an evidence collection procedure, including:
    - initiation conditions
    - actual backup procedure

  - labelling procedure
  - storage procedure
  - information procedure (under which condition which party must be informed)
  - control of the access to the evidence
  - destruction of evidence
- Obtain management sign-off of the procedure
- Advertise the existence of the procedure to all employees

5.4 Statements of applicability

In this section, we provide some statements of (non-)applicability.

Statement of applicability for "secure disposal of media" (section 8.6.2 of standard)

The security control "secure disposal of media" is applicable to our ISMS, as it covers the handling of backup tapes, which are in turn an essential part of the system under study. A wrong disposal of these tapes would lead to a breach of confidentiality of the data stored on the SAN, which is definitely not wanted.

Statement of exclusion for "Authorisation process for information processing facilities" (section 4.1.4 of standard)[5]

This R&D group made the choice of allowing more liberty for its users, in order to encourage experimentation and innovation. It is therefore unrealistic to require approval for any HW and Software changes. A couple of rules to follow have been included in the security directive in order to keep it under a minimal control.

Statement of exclusion for "Network Controls" (section 8.5.1 of standard)[6]

This control is out of scope of our ISMS, as we are considering the management of the SAN only, not the management of the intranet where it is installed.

[5] From [2]: "Whether there is a management authorisation process in place for any new information processing facility. This should include all new facilities such as hardware and software."
[6] From [2]: "Whether effective operational controls such as separate network and system administration facilities were be established where necessary. Whether responsibilities and procedures for management of remote equipment, including equipment in user areas were established. Whether there exist any special controls to safeguard confidentiality and integrity of data processing over the public network and to protect the connected systems. Example: Virtual Private Networks, other encryption and hashing mechanisms etc…"

6 Part Four: Check

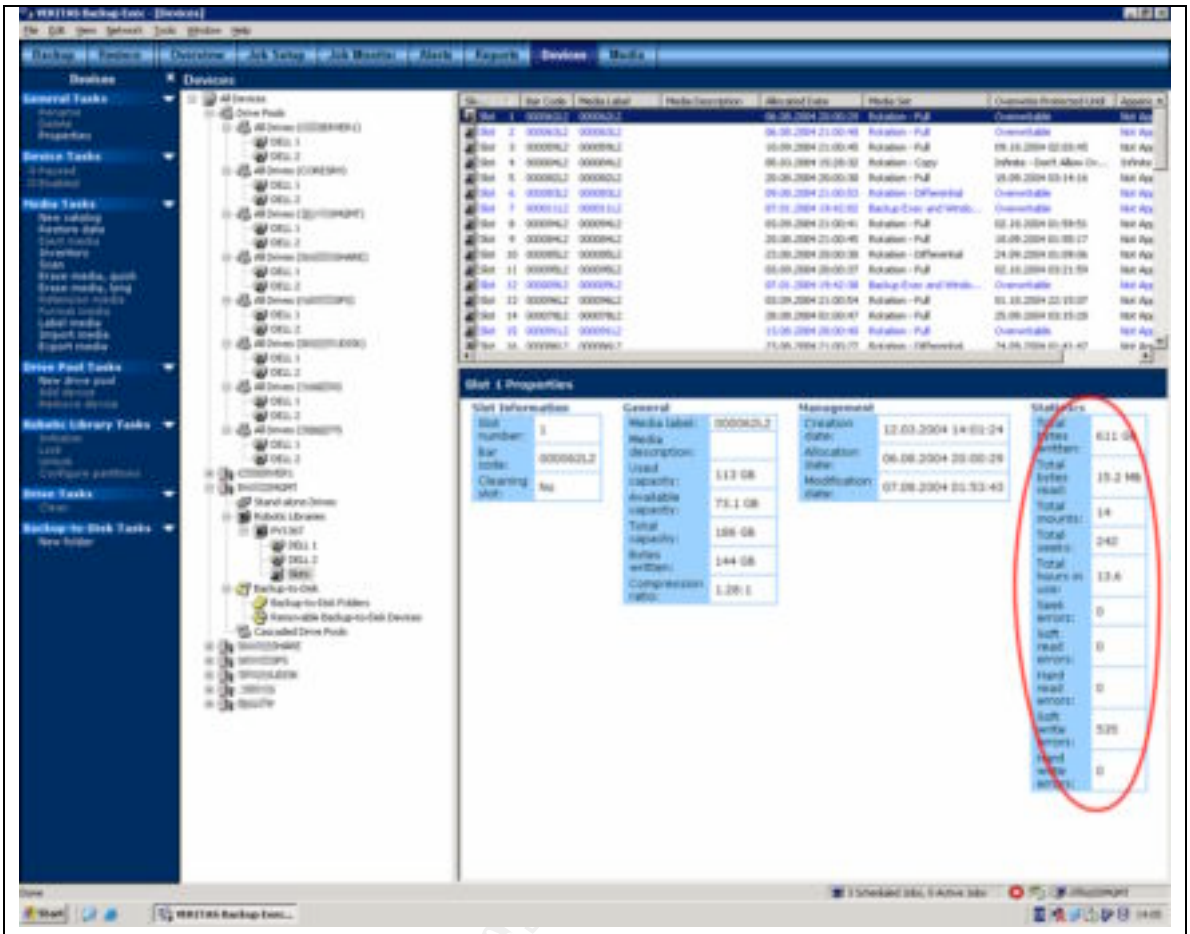
Again, in an attempt to keep consistency throughout this document, we will in this Section describe audit checklists for the three controls defined in section 4.3.1 and detailed in sections 4.4 and 5.

These checklists will be used to follow the progress of the implementation of the ISMS, and to audit this same implementation regularly. This ensures that the ISMS and its implementation are in sync.

6.1 Audit checklist for "secure disposal of media"

Audit item	"Secure disposal of Tapes" process exists and is known
Security Control objective and importance to the system	
The objective of this control is to ensure that an appropriate process has been developed and that the SAN backup manager knows it. Without such a process, it would be possible for un-wiped tapes to end up in the trash, leading to information disclosure.	
Compliance test	
Ask the SAN backup manager to show the process and to describe the content.	
Compliance requirements	
The SAN backup manager can readily provide the document, and is able to explain what its content is.	

Audit item	All existing tapes inside the tape library have not reached their end of life
Security Control objective and importance to the system	
If the process is run correctly, no tape in the library should have reached its end of life. A too old tape jeopardizes the backup process, and is a telltale sign that this process is not followed. Other elements of the process may therefore also be failing.	
Compliance test	
Check on the Veritas GUI, under the Device tab, that all registered tapes are under the "end of life" limits given in the process.	



Compliance requirements
All tapes must have statistics below the thresholds defined in the process.

Audit item	Wiping procedure is known and tested
Security Control objective and importance to the system	
Once a tape is disposed, it must be first wiped. The process for wiping must be defined and tested. If the procedure is not known, there is low chance that it is actually performed.	
Compliance test	
Ask the SAN backup manager to demonstrate the wiping procedure on an unused tape.	
Compliance requirements	
The SAN backup manager knows the procedure, and a test with an unused tape shows that previous data is effectively wiped.	

6.2 Audit checklist for "Business continuity management"

Audit item	The procedures of Business Continuity exist and are known
Security Control objective and importance to the system	
For a BCP to be successful, it must of course exist and must be known by the system managers. Without such documented procedures, you can just hope for the best, which is often not enough.	
Compliance test	
Ask the SAN Manager to show you the BCP and to describe the main elements.	
Compliance requirements	
The SAN manager is able to readily show you a paper version of the document (i.e. not stored on the SAN itself), and explains rapidly the main elements of the procedure.	

Audit item	The BCP is regularly reviewed
Security Control objective and importance to the system	
It is important that a BCP is regularly reviewed in regard to the business objectives of the system to safeguard. Failing to do so could lead to a BCP which is not applicable to the system, or that fails short of (new) business requirements.	
Compliance test	
A review team must be defined, and each member must know that there is a review of the BCP planned at least once a year.	
Compliance requirements	
The SAN manager is able to show the names of the member of the review team as well as the responsible for organizing the review. A review log must be available too, showing that such a review took place at least once a year.	

Audit item	The BCP is regularly tested
Security Control objective and importance to the system	
Ensure that the planned BCP is actually performing as expected, and that all involved personal knows the procedures. It is only possible to trust a BCP once it has been tested, and in the event of a real emergency, only trained procedures can be rolled out smoothly.	
Compliance test	
The SAN manager must organize at least once a year a complete rehearsal of the BCP. Each test must be documented.	

Compliance requirements
The SAN manager can show the reports of previous BCP rehearsals. He can indicate when will be the next test, and can show appropriate management commitment (resources).

6.3 Audit checklist for "Collection of evidence in case of suspected policy or law breach"

Audit item	The process to collect evidence exists and is known
Security Control objective and importance to the system	
The objective of this control is to ensure a proper process for collecting and preserving evidence has been designed and is known from all involved personal.	
Compliance test	
Obtain the documented process (either by asking Human Resources, Security Manager, or the SAN manager), and ask all mentioned personal to describe the main elements of the procedure.	
Compliance requirements	
The documented process must describe who can initiate the process, but this will typically be Human Resources, under the supervision of the Security Manager. The SAN manager must know the actual procedure for collecting, backing up, securely storing, and destroying the data. The procedure must include the provision of an action log (to be filled by all parties).	

Audit item	Legal review of the evidence collection process
Security Control objective and importance to the system	
The objective of this control is to ensure that the evidence collection process doesn't breach any data privacy law. It ensures that the evidence will be receivable by a court in case of legal procedures.	
Compliance test	
Check if the procedure has been reviewed by a legal advisor, or instruct to have such an assessment performed.	
Compliance requirements	
The legal review must show no breach of law, or give constraints to be followed during the procedure. (One such constraint would be a maximum storage time, especially if the suspicions prove to be unfounded).	

7 Part Five: Act

A very important part of the ISMS is to keep it “alive”. This includes regular review and audits, as well as collection of actual operational events relevant for the ISMS.

The data collected during these reviews or through daily use of the ISMS must flow into a process which goal is to continually adapt the ISMS.

The following sections describe these two aspects of the maintenance of the ISMS.

7.1 Reviews and audits

We have seen that many requirements or security controls of the SAN system derives from business objectives. As these objectives may change along the development of the organisation, it is important to review regularly all implemented controls to ensure their fitness to the business.

This review process will take place continually through the year, and will be performed by the security team. This team meets already once a month, and can add this task to its agenda.

The security team will essentially review potential changes due to business changes. The SAN manager will review on its own the ISMS and request review for specific sections to the security team.

The review activity must be documented (review log), at best by documenting the reviews in the ISMS sections themselves.

The whole ISMS must be audited too, in more details. Such an audit must be performed by an external entity, and will verify that the ISMS fits the business objectives, and that it is “lived” by the involved personal.

No specific schedule for such large audits is specified, but it should occur at least once every two years.

The audit activity must be documented (audit log) in separate documents, and kept with the ISMS.

During the operation of the ISMS, it is possible that either security incidents occur, or that simply some designed security controls are unpractical.

This information must be recorded and documented, either by the SAN manager itself, or by the security manager. These documents must be kept along the ISMS.

7.2 ISMS maintenance

The output of the reviews, audits or operational events must initiate a modification of the ISMS if necessary.

The security team design a task responsible that has to integrate the new information in the appropriate ISMS elements. He/she can be helped in this task by other members of the security team, or by the SAN manager. A deadline for a change proposal is also defined.

If the change is important, it must be signed-off by management. This gives also the opportunity to request additional means or resources to implement the modification.

Finally, the change is implemented.

Figure 8 shows this process.

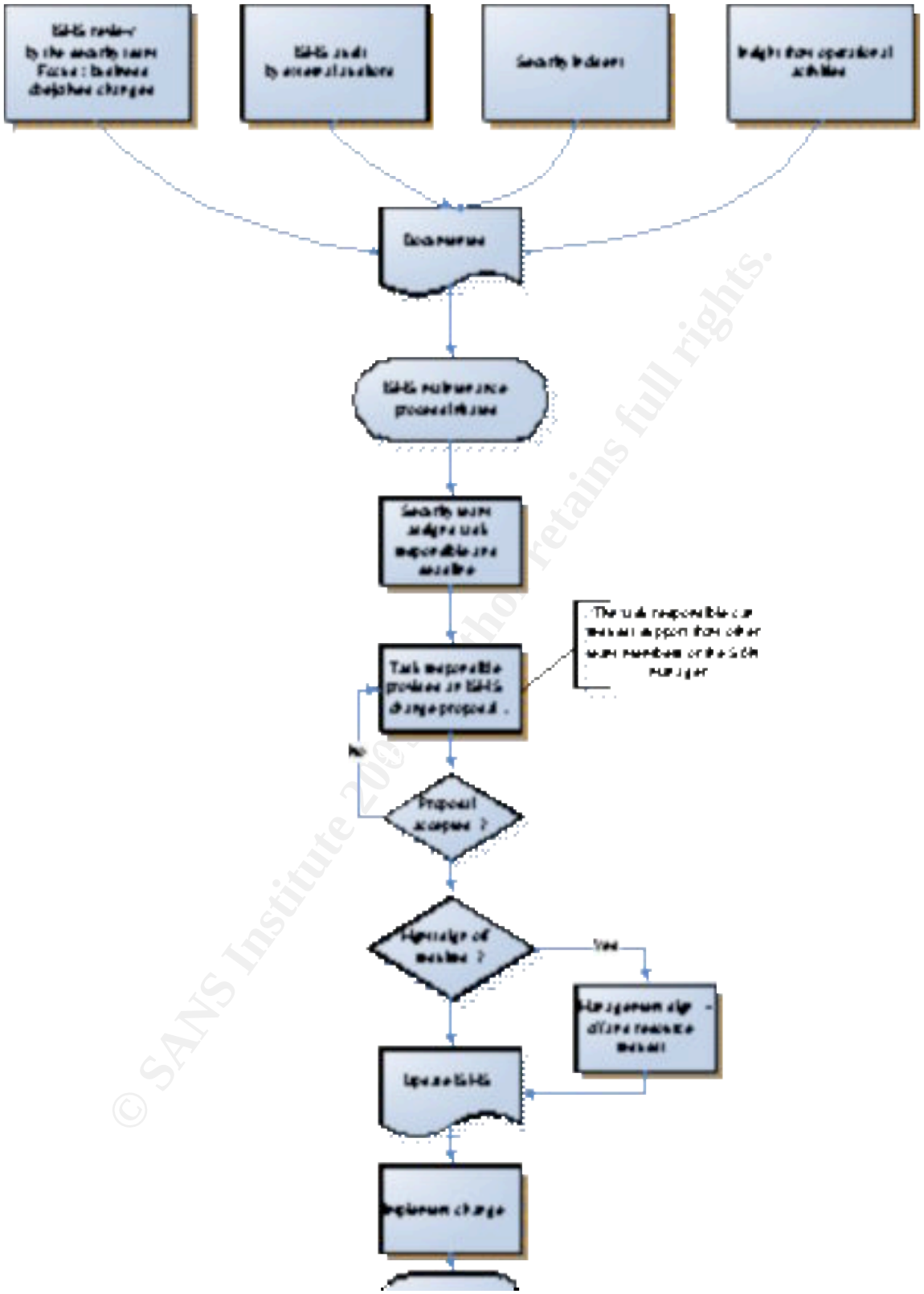


Figure 8: ISMS maintenance process

8 References

[1] Microsoft. “SharePoint Portal Server”. URL: http://office.microsoft.com/home/office.aspx?assetid=FX010909721033 (9.9.2004)

[2] Thiagarajan, Valliappan. “ISO 17799 Checklist 1.1”. SANS SCORE project. Version 1.1. August 6 2003. URL: http://www.sans.org/score/checklists/ISO_17799_checklist.doc (9.9.2004)

[3] British Standard, “Information technology Code of practice for information security management”, BS ISO/IEC 17799:2000, February 2001, ISBN 0 580 36958 7

[4] Quantum Corporation, “DLT tape FAQ”, 2004, URL: http://www.dlttape.com/DLTtape/Products/Media/Media+FAQ.htm (19.9.2004)