

Security Governance Master of Science in Cyber Security

AA 2023/2024

A MODEL FOR INFORMATION SECURITY GOVERNANCE

Recap on Information Security Governance

In NIST SP 800-100, Information Security Governance is defined as

- *“The process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.”*

Said differently, ISG is the global effort needed to ensure the well-being of the company's electronic resources.

Recap on Information Security Governance

ISG must ensure cost-effectiveness

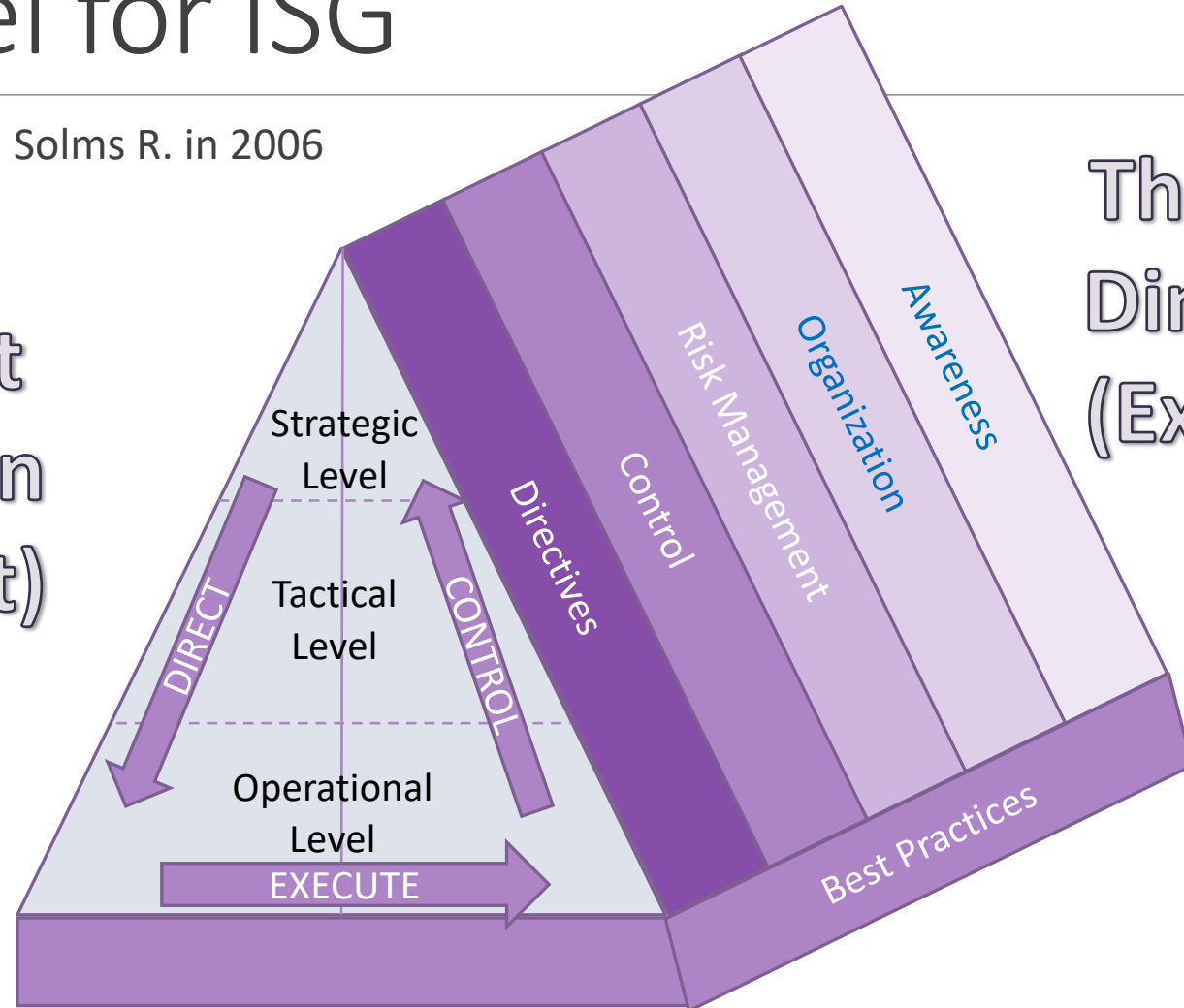
- There must be a balance between the cost of protecting electronic resources and the risk to which these resources are exposed
- NO OVERPROTECTION causing unnecessary expenses
- NO UNDERPROTECTION causing risk to materialize and impact the company

A good (IT) Risk management strategy is therefore mandatory to implement a good ISG strategy

A Model for ISG

Introduced by Von Solms R. in 2006

The Front
Dimension
(Core Part)



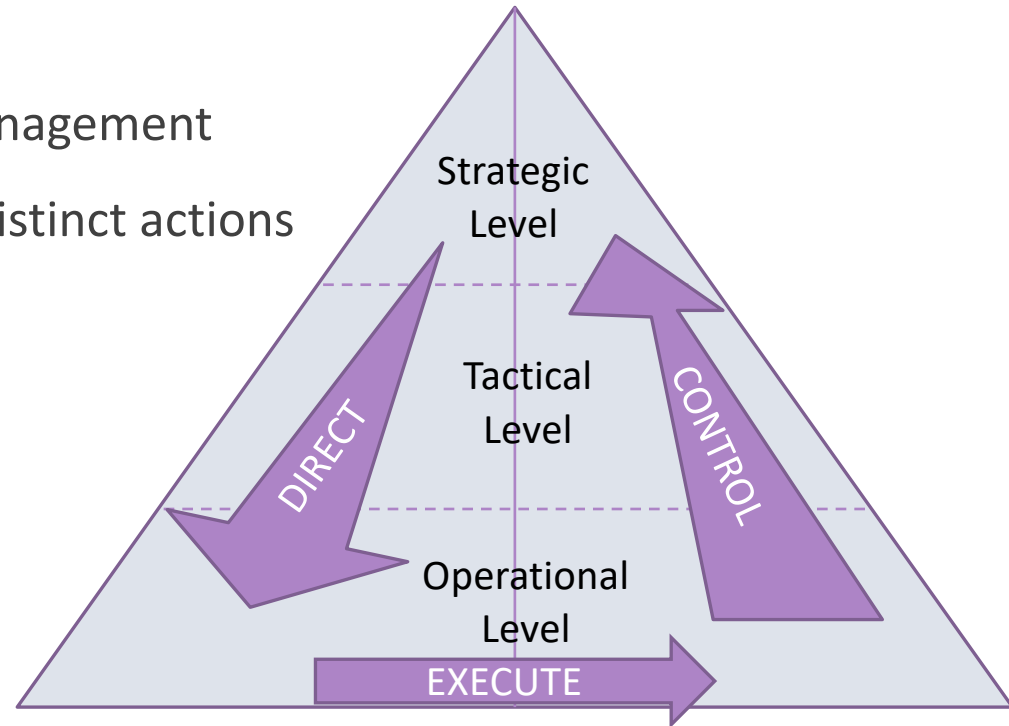
The Depth
Dimension
(Expanded
Part)

The Front Dimension (Core Part)

It represents the execution of processes and actions and the influence of the Direct and Control loop on these processes.

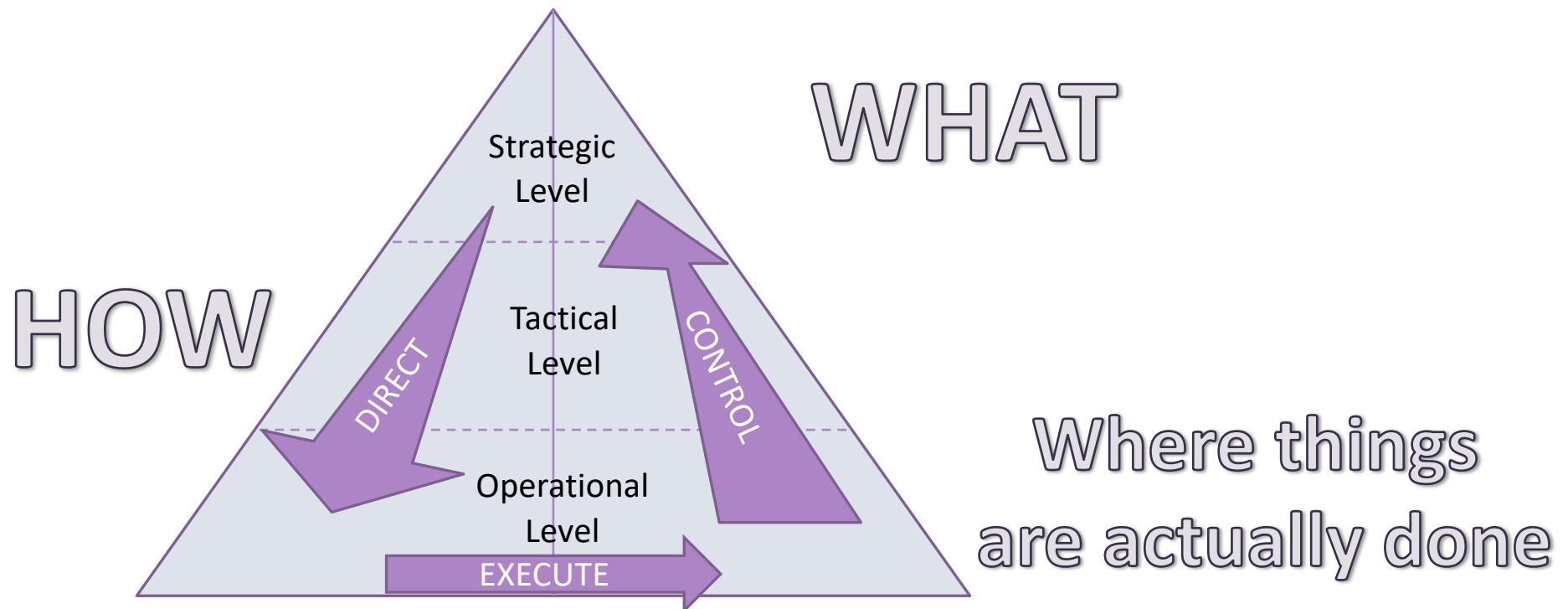
It is based on two core principles:

1. It covers the 3 well known level of management
2. Across these 3 levels, there are very distinct actions



Core Principle 1

The Model covers the three well-known levels of management: Strategic, Tactical and Operational.

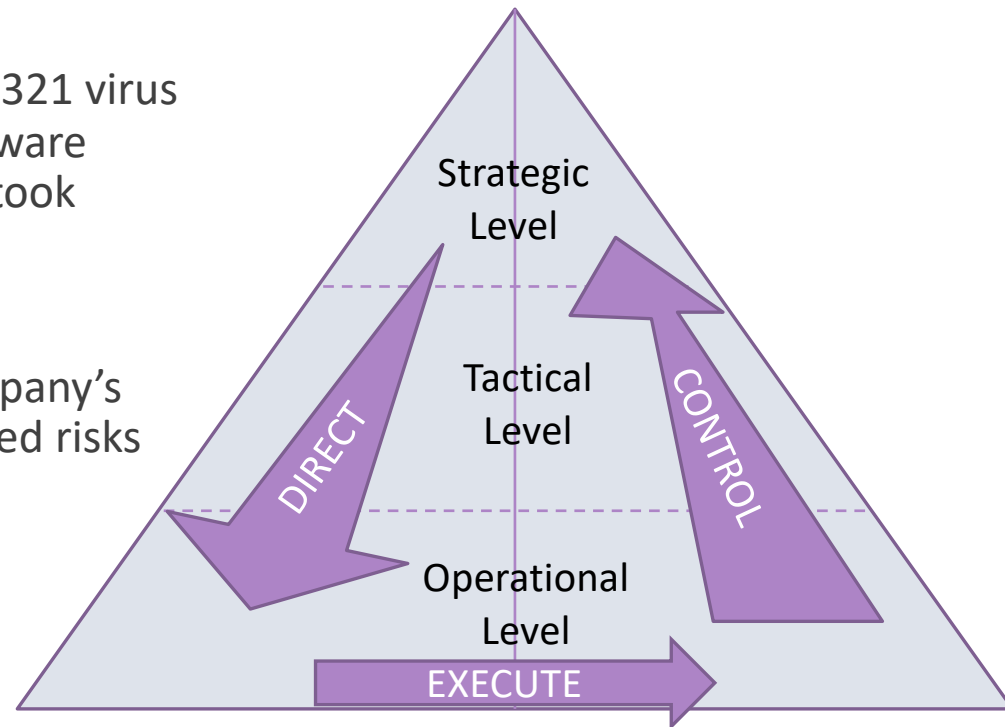


Core Principle 2

Across these three levels, there are three very distinct “actions”

Rational

- the Board is not interested in knowing that 321 virus attacks occurred last week and that 27 software patched and 7 anti-virus software updates took place (Too much details to plan)
- The Board wants to know whether the company's access to the internet causes any unmitigated risks to the company.
 - If not, it is happy 😊
 - if so, it wants to know about such unmitigated risks



The *Direct* Part

	STRATEGIC	TACTICAL	OPERATIONAL
What does it mean Direct at this level	Identify assets, their relevance and their required level of protection	Directives are 'expanded' into sets of relevant information security policies, company standards and procedures	Inputs are expanded into sets of administrative guidelines and administrative procedures and technical measures are physically implemented and managed
INPUT	<ul style="list-style-type: none"> External factors (legal and regulatory prescriptions and other external risks) Internal factors (company's strategic vision, IT role, competitiveness, etc) 		
OUTPUT	<ul style="list-style-type: none"> a set of Directives indicating (at high level) what the Board expects must be done as far as the protection of the company's information assets is concerned 	<ul style="list-style-type: none"> policies, procedures and standards 	<ul style="list-style-type: none"> operating procedures specifying how things must be done. It forms the basis of execution on the lowest level

The *Control* Part


“you can only manage what you can measure”

- To properly Control (manage) we need to measure...
- to measure, we need to know which information and data to collect

This ‘measurability’ characteristic must be at the centre of all directives, policies, standards and procedures produced during the ‘Direct’ part of the model

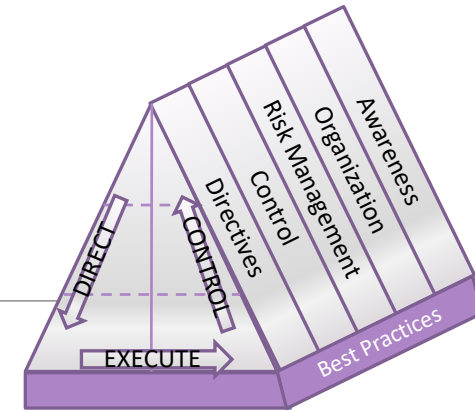
The *Control* Part

	OPERATIONAL	TACTICAL	STRATEGICAL
What does it mean Control at this level	measurement data is extracted from a wide range of entities (either automatically or manually)	measurement and monitoring against the requirements of the relevant policies, procedures and standards	Situational Awareness
INPUT	Measurements		
OUTPUT	Specialized reports can be created on this level using this extracted operational data.	Tactical Management reports, indicating levels of compliance and conformance	Reports reflecting compliance and conformance to relevant directives including risk considerations



The diagram illustrates the flow of data and information across the three levels of control. A purple arrow points from the 'INPUT' row of the 'OPERATIONAL' column to the 'TACTICAL' column. Another purple arrow points from the 'OUTPUT' row of the 'TACTICAL' column to the 'STRATEGICAL' column.

Best Practices



RECALL: ISG model should help in “doing the right things right”

Thus, every Information Security Manager (ISM) must be able to answer to the following questions:

1. How do I know what the right things are?
2. Suppose that I know, how do I know I am doing right?

Look to Best Practices

What is a Best Practice?

Best Practices (or Standards or Guidelines) are a set of documents reporting experiences and solutions experienced by experts in ISM

- Can be seen as the consensus of experts in the field of Information Security
- Provide an internationally accepted framework that can be used as building block for ISG.

Many of them exists, focused on related but different aspects

- ISO 27000 family
- COBIT
- NIST SP 800-*
- CSC
- NIST CSF
- ...

ISO 27002

It is an International Standard designed to be used by organizations that intend to:

- a) select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;
- b) implement commonly accepted information security controls;
- c) develop their own information security management guidelines.

BS ISO/IEC 27002:2013
ISO/IEC 27002:2013(E)

It contains 14 security control clauses collectively containing a total of 35 main security categories and 114 controls.

Contents	Page
Foreword	v
0 Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Structure of this standard	1
4.1 Clauses	1
4.2 Control categories	1
5 Information security policies	2
5.1 Management direction for information security	2
6 Organization of information security	4
6.1 Internal organization	4
6.2 Mobile devices and teleworking	6
7 Human resource security	9
7.1 Prior to employment	9
7.2 During employment	10
7.3 Termination and change of employment	13

ISO 27002

Each clause defining security controls contains one or more main security categories

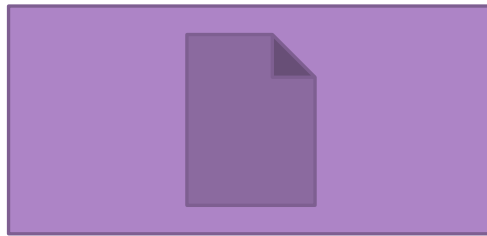
Each main category contains:

1. a) a control objective stating what needs to be achieved
2. b) one or more controls that can be applied to achieve the control objective

Control descriptions are structured as follows

Control	Defines the specific control statement, to satisfy the control objective.
Implementation Guidance	Provides more detailed information to support the implementation of the control and meeting the control objective. The guidance may not be entirely suitable or sufficient in all situations and may not fulfil the organization's specific control requirements.
Other Information	Provides further information that may need to be considered, for example legal considerations and references to other standards. If there is no other information to be provided this part is not shown.

ISO 27002 - Example



Ref. ISO/IEC 27002:2013

ISO 27001

It is an International Standard and specifies the requirements for establishing, implementing, maintaining and continually improving an ISMS within the context of the organization

It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization

It is generic and intended to be applicable to all organizations, regardless of type, size or nature.

ISO 27001 and ISO 27002

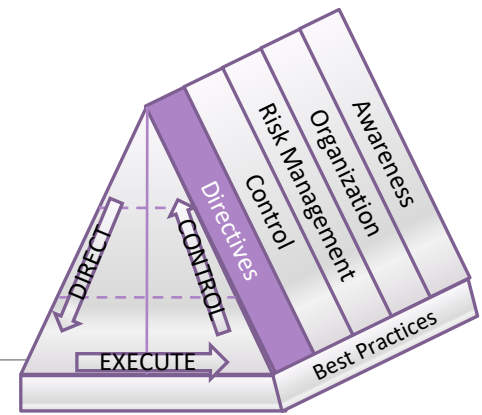
ISO 27001

- very specific and strict, and spells out, in detail, what a company must comply with and have in place to be formally certified.

ISO 27002

- is a 'guideline' document, and advises companies on what they should have in place as far as their Information Security Management is concerned, in order to follow 'Best Practice'
- guides a company to structure its Information Security Management according to the experience of other companies
- rather high level, and does not drill down to very detailed specifics.

Directive



Security Policy documents are required from Standards and Best Practices

E.g., From ISO 27002 we have

5 Information security policies

5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1.1 Policies for information security

Control

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

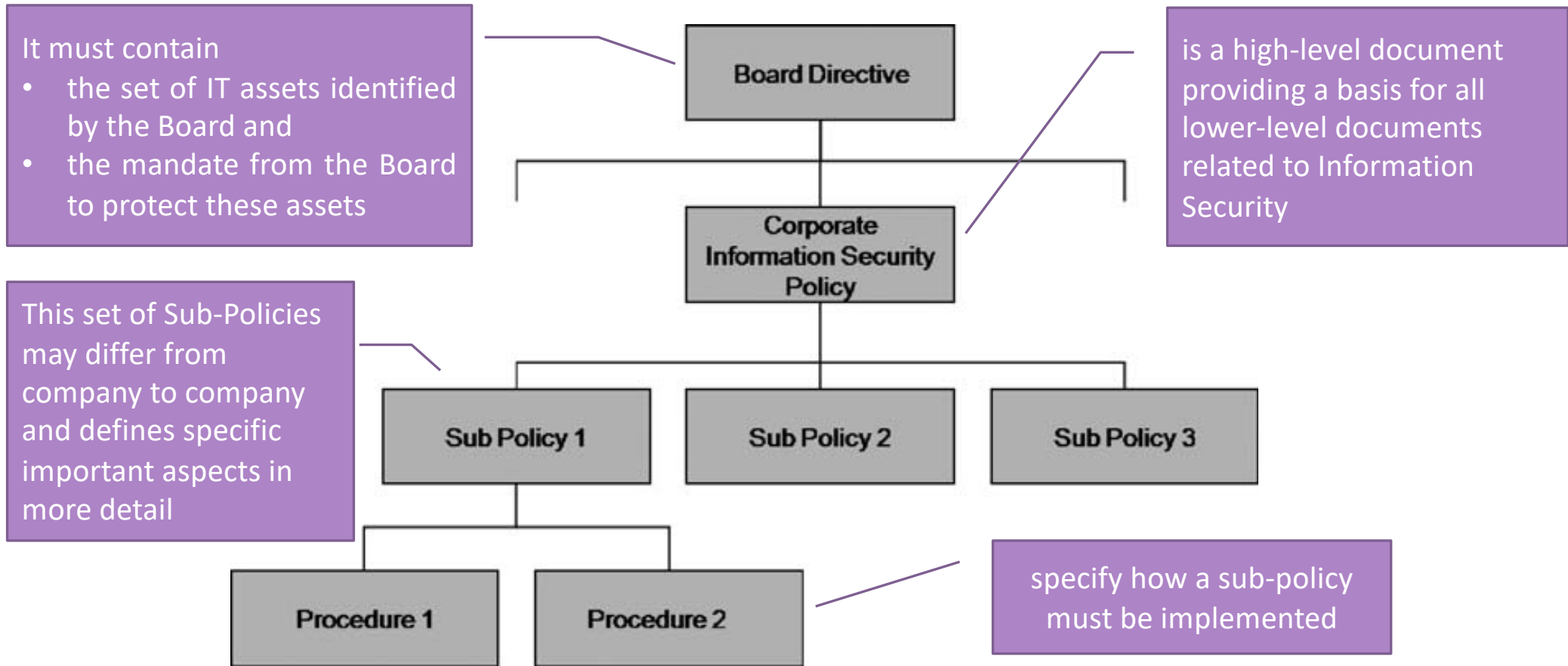
An Information Security Policy Architecture (ISPA) and related Documents

In order to comply with the requirements of having a documented Direct process, it is important to define a methodology to create, manage and distribute policy related documents.

We will consider the following set of documents as component of an ISPA

- A Board-initiated Directive concerning Information Security Governance
- A Corporate Information Security Policy (CISP) flowing from the Directive
- A set of detailed sub-policies flowing from the CISP
- A set of company standards based on the Corporate and Detailed Policies
- A set of administrative and operational procedures, again flowing from the detailed set of sub-policies

ISPA



The Corporate Information Security Policy (CISP)

Guidelines to create a proper CISP:

1. The CISP must indicate Board and executive management support and commitment and it must be clear that the CISP flows from a higher-level directive
2. The CISP must be accepted and signed by the CEO or equivalent officer
3. The CISP must not be a long document, nor must it be written in a technical form. The maximum length should be about four to five pages, and it must contain high-level statements concerning Information Security
4. The CISP should not change very often, and must be 'stable' as far as technical developments and changes are concerned
5. For the reason mentioned above, the CISP must not contain any references to specific technologies, and must be 'technology neutral'

The Corporate Information Security Policy (CISP)

Guidelines to create a proper CISP:

6. The CISP must indicate who is the owner of the Policy and what the responsibilities of other relevant people are
7. The CISP must clearly indicate the Scope of the Policy, that is, all people who will be subject to the Policy
8. The CISP must refer to possible (disciplinary) actions for non-conformance to the it and its lower-level constituent policies
9. The CISP must be distributed as widely as possible in the company and must be covered in all relevant awareness courses
10. The CISP must have a Compliance Clause

CISP Example

The XXX Corporate Information Security Policy

Final Version: (date)

Review Date: (date)

Author: <Name 1>

Owner: <Name 2>

Contents

- 1. The importance of information to XXX**
- 2. What is Information Security?**
- 3. Why XXX needs Information Security**
- 4. The Information Security Commitment of XXX's Board**
- 5. Scope**
- 6. Information Security Statements in this Corporate Information Security Policy**
- 7. Responsibilities**
- 8. Compliance Clause <to be discussed in the next chapter>**

CISP Example

5. Scope

This Policy applies to:

- 5.1 All XXX's IT assets stored, processed and distributed via XXX's information processing systems;
- 5.2 Any person who had been granted authorization to access XXX's IT resources, including, but not limited to, permanent, temporary, third party, contractual employees and users;
- 5.3 All business partners and clients that access XXX's IT assets in any way.

6. Information Security Statements in this Corporate Information Security Policy

Statement 6.1

XXX will have a proper Information Security organizational structure to manage Information Security according to this Corporate Information Security Policy and its constituent sub-policies.

This structure will:

- ensure that security roles be assigned to all users;
- that all users are aware of the content of this Policy;
- that all users are aware of the disciplinary consequences of not complying with this Policy;
- coordinate and review the continuous implementation of this Policy.

Statement 6.2

All IT assets in XXX will have a documented way in which they are handled, including:

- being reflected in a company-wide inventory;
- having a nominated owner who will ensure proper rules for the handling and protection of such assets.

7. Responsibilities

- 7.1 Senior Management
- 7.2 Information Security Manager
- 7.3 Business Systems' Owners
- 7.4 Risk Management/Audit Department
- 7.5 User

Sub-policies

The set of Sub-Policies may differ from company to company, but usually the following ones will be defined for everybody:

- A Malicious Software Control Policy (Anti-Virus Policy)
- An Acceptable Internet Usage Policy
- An Acceptable Email Usage Policy
- A Logical Access Control Policy
- A Disaster Recovery (Backup) Policy
- A Remote Access Control Policy
- A Third Party Access Control Policy



IMPORTANT

It is very important that the ISPA clearly indicate where these different policies originate

- this means that any sub-policy must be 'linked' or 'traced back' to the CISP in some way

Sub-policy Example

The XXX Internet Acceptable Use Information Security Policy

Final Version: (date)

Review Date: (date)

Author: <name 1>

1. Introduction

XXX currently supplies an Internet access service that is available to all authorized XXX and

3. Reference

3.1 Up

Statements 6.5 and 6.6 in XXX's Corporate Information Security Policy give origin to this Sub-Policy.

3.2 Down

The following lower level procedure supports this Sub-Policy.
'Application Procedure for XXX Internet Service Connectivity'

5. Main Policy Statement

Use of the XXX Internet Service must be in support of official XXX work or activities.

Sub-Statements supporting the main Statement

Statement 5.1

Use of the XXX Internet Service must be in support of official XXX work or activities. All user requests for XXX Internet Service connectivity must be approved and supported by the employee's line Manager. Requests for Internet Service must be done using the specified procedure 'Application Procedure for XXX Internet Service Connectivity'.

Statement 5.2

It will be the responsibility of the user's line Manager to ensure that the user does not misuse the Internet Service.

Procedure Example

The XXX Application Procedure for Internet Service Connectivity

Final Version: (date)

Review Date: (date)

Author: <Name 1>

Owner: < Name 2>

This Procedure follows from Statement 5.1 in XXX's Internet Acceptable Use Information Security Policy.

1. Surname :
2. Initials :
3. Department :
4. Office number :
5. Telephone extension :
6. Home phone number :

I have read XXX's Corporate Information Security Policy, as well as the XXX Internet Acceptable Use Information Security Policy. I understand the content, and if access is granted to me, I will use it in line with these stated Policies.

Signature of Applicant :

Date :

I am satisfied that the applicant needs the access applied for, and that the applicant is aware of the policies governing the specific access

Line Manager's Signature :

Date :

Information Security Officer's Signature :

Date :

Compliance Clause : <to be discussed in the next chapter>

Control

Compliance check is the main scope of the Control part of the model.

In ISO 27002 it clearly required with the following controls:

18 Compliance

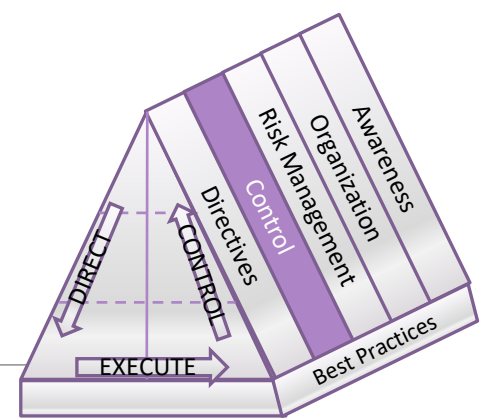
18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

18.2.2 Compliance with security policies and standards

Control

Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.



Problem:
how compliance clauses
for ISPA documents can be
defined?

Compliance Clauses

Recall: You can assess only what you can measure

Thus... Compliance clauses need to provide a clear metric that can be evaluated and assessed

Traditionally, Compliance monitoring is done by performing periodic ICT Audit sessions

- ICT risks are evaluated
- An audit report is produced and its results compared with compliances clauses

ISSUES

- Timing is a crucial factor
- The world is dynamic and monitoring should be done in near real time

Compliance Clauses

Unfortunately, specifying compliance clauses is not an exact science and very few guidelines are available

Some of them are:

- Compliance Clauses must be clear and precise
 - e.g., a clause like “Employees must take Information Security seriously” is vague... What does it mean “seriously”?
- Compliance Clauses should express a way to measure its satisfaction

Example of Clause for the Board Directive

Let us consider the following extract from a Board Directive

The Board of XXX accepts the importance of the company's IT infrastructure in furthering the strategic goals of the company. The Board also realizes the potential impact it can have on the company, and the consequences to the company if this IT infrastructure is compromised in any way. For this reason, the Board demands a proper environment to protect the IT infrastructure against any disruptions or compromises.

The Board fully supports a proper ISG environment for XXX.

Option 1

Compliance Clause:

The Board requires a proper feedback, every three months, of the level of compliance with this Directive.

Option 2

Compliance Clause:

The Board requires a detailed feedback, every three months, of any serious risks which may compromise the protection of XXX's ICT infrastructure.

Example of Clauses for CISP

Recall: CISP is generally articulated in several Statement

6. Information Security Statements in this Corporate Information Security Policy

Statement 6.1

XXX will have a proper Information Security organizational structure to manage Information Security according to this Corporate Information Security Policy and its constituent sub-policies.

This structure will:

- ensure that security roles be assigned to all users;
- that all users are aware of the content of this Policy;
- that all users are aware of the disciplinary consequences of not complying with this Policy;
- coordinate and review the continuous implementation of this Policy.

Statement 6.2

All IT assets in XXX will have a documented way in which they are handled, including:

- being reflected in a company-wide inventory;
- having a nominated owner who will ensure proper rules for the handling and protection of such assets.

It would be preferable to have a compliance clause for each statement

Example of Clauses for CISP

6. Information Security Statements in this Corporate Information Security Policy

Statement 6.1

XXX will have a proper Information Security organizational structure to manage Information Security according to this Corporate Information Security Policy and its constituent sub-policies.

This structure will:

- ensure that security roles be assigned to all users;
- that all users are aware of the content of this Policy;
- that all users are aware of the disciplinary consequences of not complying with this Policy;
- coordinate and review the continuous implementation of this Policy.

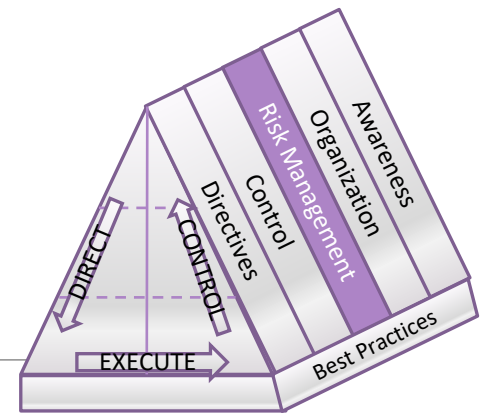
Option 1

The effectiveness of XXX's Information Security organizational structure in managing and enforcing the requirements of the company's ISPA shall be evaluated every six months and the results incorporated in higher-level reporting.

Option 2

The way the Information Security function in XXX is organized, and the reporting structures within this function shall be evaluated every 12 months to ensure that the structure stays adequate to ensure the proper protection of all the electronic assets of XXX. The results of this evaluation will be part of the annual evaluation and reporting of organizational structures in the company.

Risk Management



Risk Management is the process to identify and assess all potential risks as well as introducing controls that should mitigate all these risks to acceptable low levels.

Today, in most circumstances, risk has two factors associated with it:

- a probability or frequency
- a magnitude of gains or losses (impact)

Thus, the aim of risk management is to determine

1. what the impact will be if the risk does materialize and
2. how often (probability or frequency) this risk might materialize

EXAMPLES

1. If fire destroys the entire computer centre, the impact will be serious although the probability that it might happen is fairly small
2. On the other hand, the probability that a malicious software virus might infect some business data is fairly high, but normally the impact is not serious

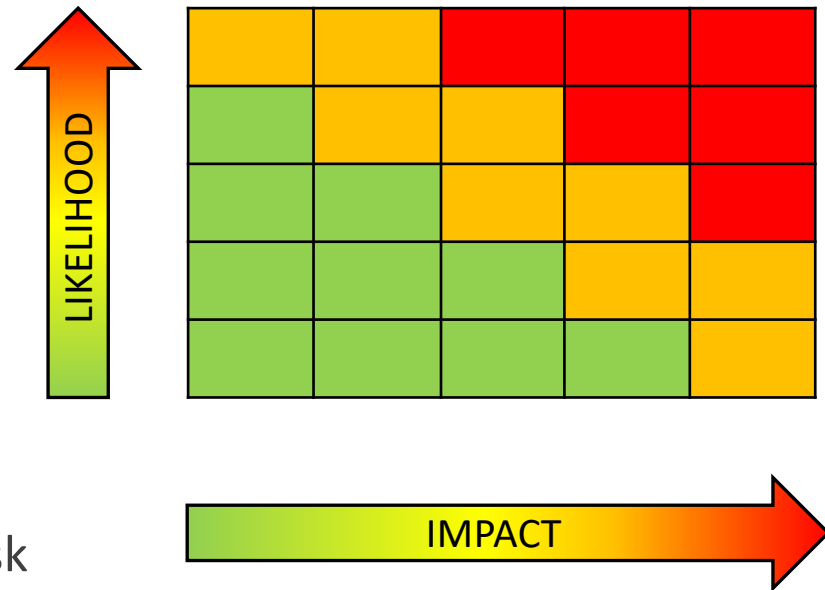
Risk and its mitigation

Risk = Likelihood * Impact

= (Threat * Probability) * Impact

How to
reduce risks?

1. Reduce the potential impact or the risk
2. Reduce the probability or frequency of the risk
3. A combination of both of the above



Risk Management and ISO 27002

ISO 27002 sees IT risk analysis as an essential part of Best Practices in IT

0.2 Information security requirements

It is essential that an organization identifies its security requirements. There are three main sources of security requirements:

- a) the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated;
- b) the legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy, and their socio-cultural environment;
- c) the set of principles, objectives and business requirements for information handling, processing, storing, communicating and archiving that an organization has developed to support its operations.

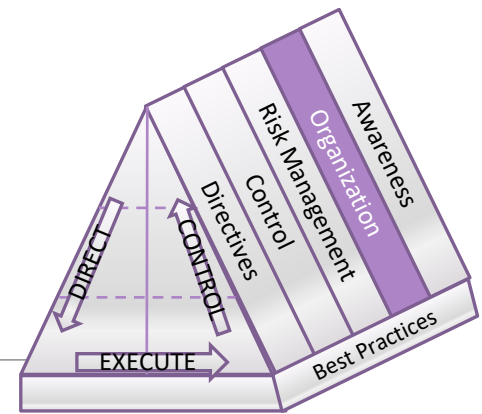
Risk Management and Governance

All risks that could possibly have a negative effect on the well-being of the organization (if and once they materialize) are definitely the responsibility of management

Thus, all levels of organizational management should be involved in the process of Risk Management

It is imperative that information and IT- related risks are managed in an integrated manner with business risks

Organization



In any company, the way Information Security is organized is very important

All Best Practice documents underline this aspect

- E.g., in ISO 27002 there is a clause titled 'Organization of Information Security'

A good approach is to have at least two distinct components in the organization

1. One looking at day-to-day operational aspects
2. One responsible for the compliance monitoring function

Information Security Operational Management

Activities included in this dimension are, for example:

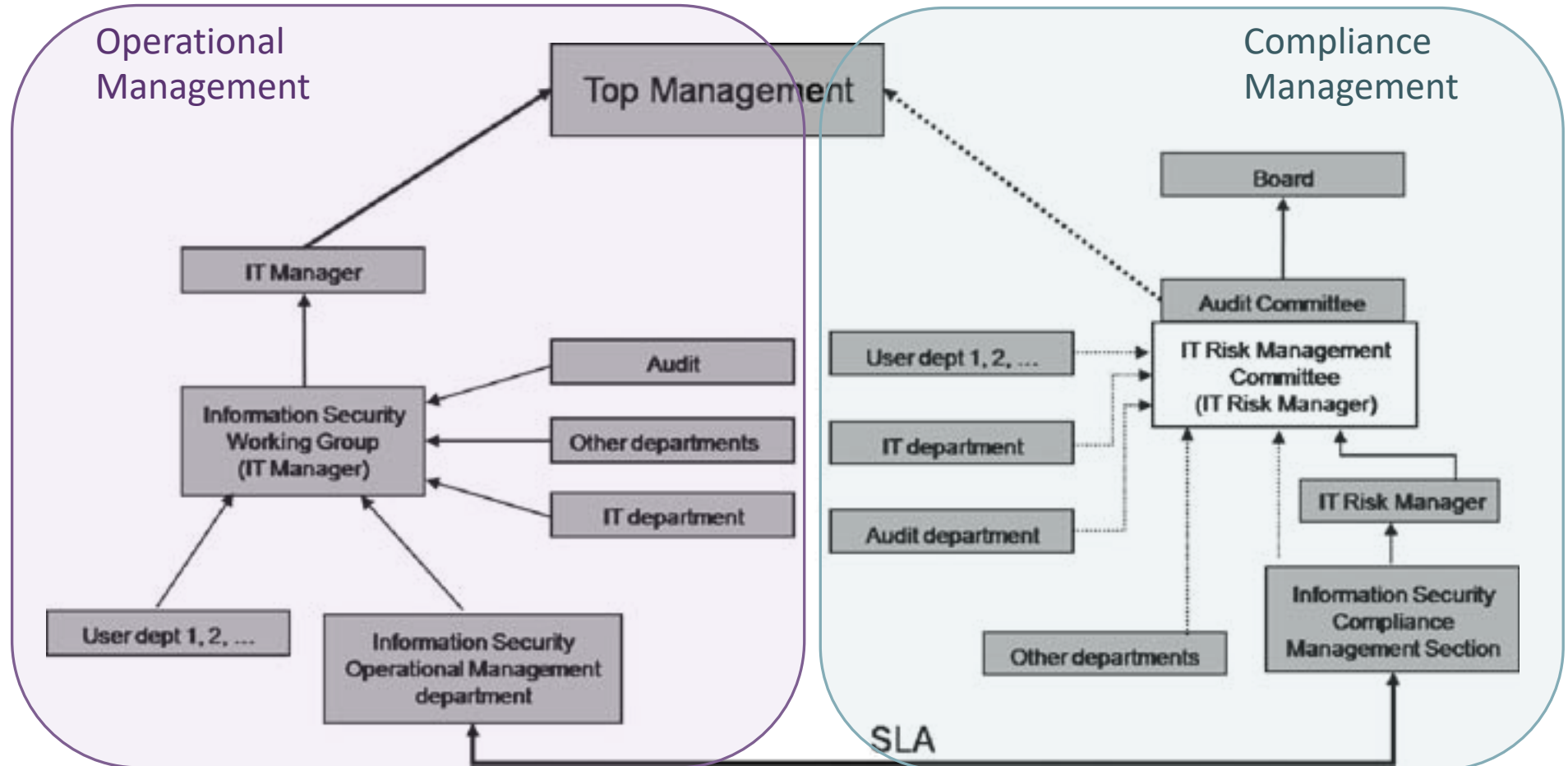
1. Logical access control management
 - i.e., the real actions of adding to, changing and deleting user access rights from access control lists, etc
2. Identification and authentication management
 1. i.e., the real actions of adding to, changing and deleting from the user ID database and password files
3. Firewall management
 1. configuring firewalls with the authorized access rights, connecting workstations to LANS and the Internet, etc
4. Virus and malicious software management
 1. i.e., installing and updating antivirus software
5. Handling antivirus and related types of security incidents
6. Setting and updating the security settings and configurations of workstations and servers
7. Ensuring availability through UPS systems
8. Ensuring backups and secure storage of backups
9. ...

Information Security Compliance Management

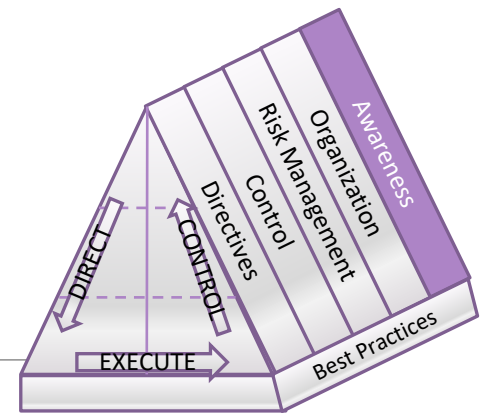
Activities which must be managed as far as compliance is concerned include:

- The level to which previously identified IT risks are managed and mediated
- The level of Information Security awareness of users
- The availability, completeness and comprehensiveness of Information Security policies, procedures and standards
- The level of compliance to such policies, procedures and standards
- The impact on the IT risk level of the company when policies are not complied with
- The compliance with regulatory, legal and statutory requirements
- Software licensing issues
- ...

Organizing Information Security Governance



Awareness



RECALL: *All the levels are involved in the ISG Process*

Information Security procedures, guidelines and practices must be drafted and conveyed to ALL users of information and IT in the organization

Thus, ALL information workers must be made aware (and trained) of the Information Security policy as well as the associated procedures, guidelines and practices

Information Security Education, Training and Awareness (SETA)

Information Security Education, Training and Awareness should be extensions of the general knowledge that employees already have to do their jobs

- The objective is to teach each of them to do their jobs securely

The objectives of a SETA Programme are to:

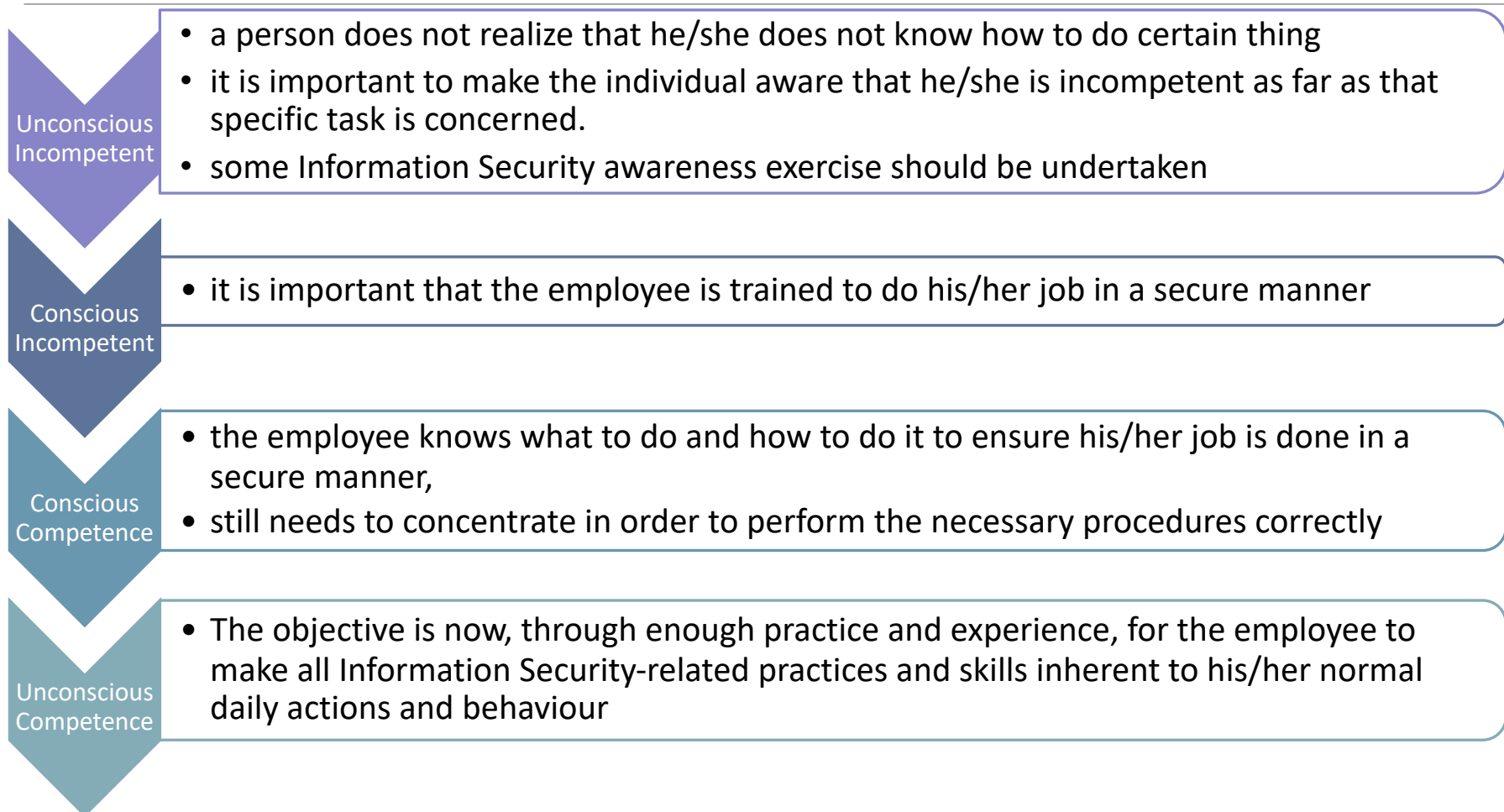
1. Improve awareness of the importance and need to protect organizational information resources
2. Acquire the necessary skills and know-how to do their jobs more securely
3. Create an understanding and insight into why it is important to protect organizational information assets

Information Security Education, Training and Awareness (SETA)

Table 10.1 Differentiation between awareness, training and education

	Awareness	Training	Education
Attribute	What	How	Why
Level	Information	Knowledge	Insight
Objective	Alert to	Skill	Understanding
Teaching method	Media <ul style="list-style-type: none">• Videos• Newsletters• Posters	Practical Instruction <ul style="list-style-type: none">• Lecture• Workshop• Hands-on practice	Theoretical Instruction <ul style="list-style-type: none">• Seminar• Literature study
Impact timeframe	Short-term	Medium-term	Long-term

The Conscious Competence Learning Model



Pillars of training

Employees must be trained about aspects such as:

- Why information is such an important asset?
- The information security policy and procedures
- The role and responsibility of every employee
- The consequences of not complying with the policy

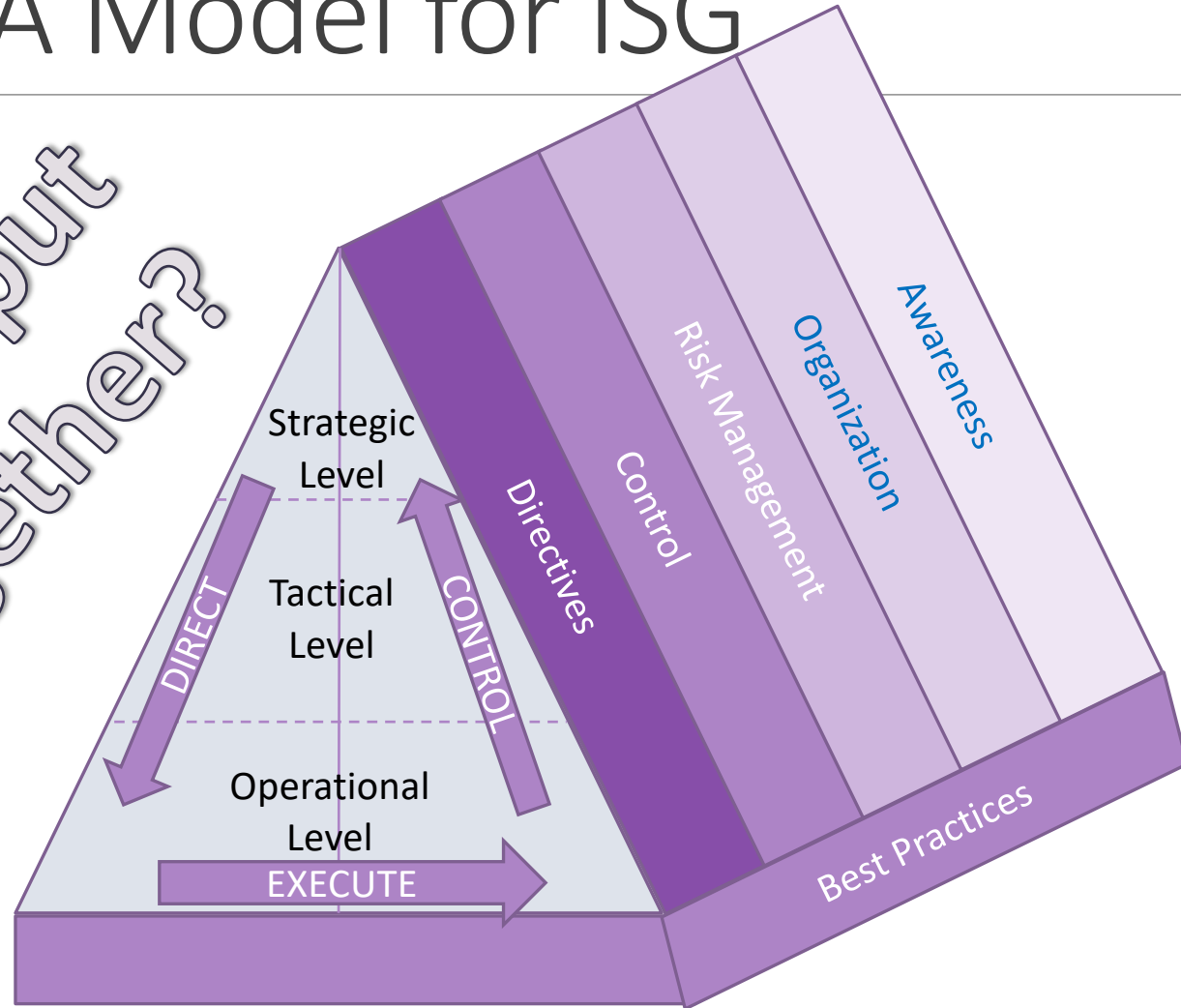
Such training should typically address issues such as:

- User identification and authentication (passwords)
- How to choose a password
- No sharing of user IDs and passwords, etc.
- Virus control
- Backing-up information
- Sharing and storing confidential information
- Secure email usage
- Secure Internet usage
- Social engineering
- Handling of mobile devices, e.g., notebooks and PDAs
- Legal usage of software
- Office manners and discipline, e.g., clean desk
- Required actions if a security incident or breach is suspected.

A Methodology for Establishing an Information Security Governance Environment

Recap: A Model for ISG

How do we put
it all together?



A high-level methodology for establishing an ISG environment

The methodology will consist of 14 steps

- 9 setup steps
- 5 steps in continuous cycle

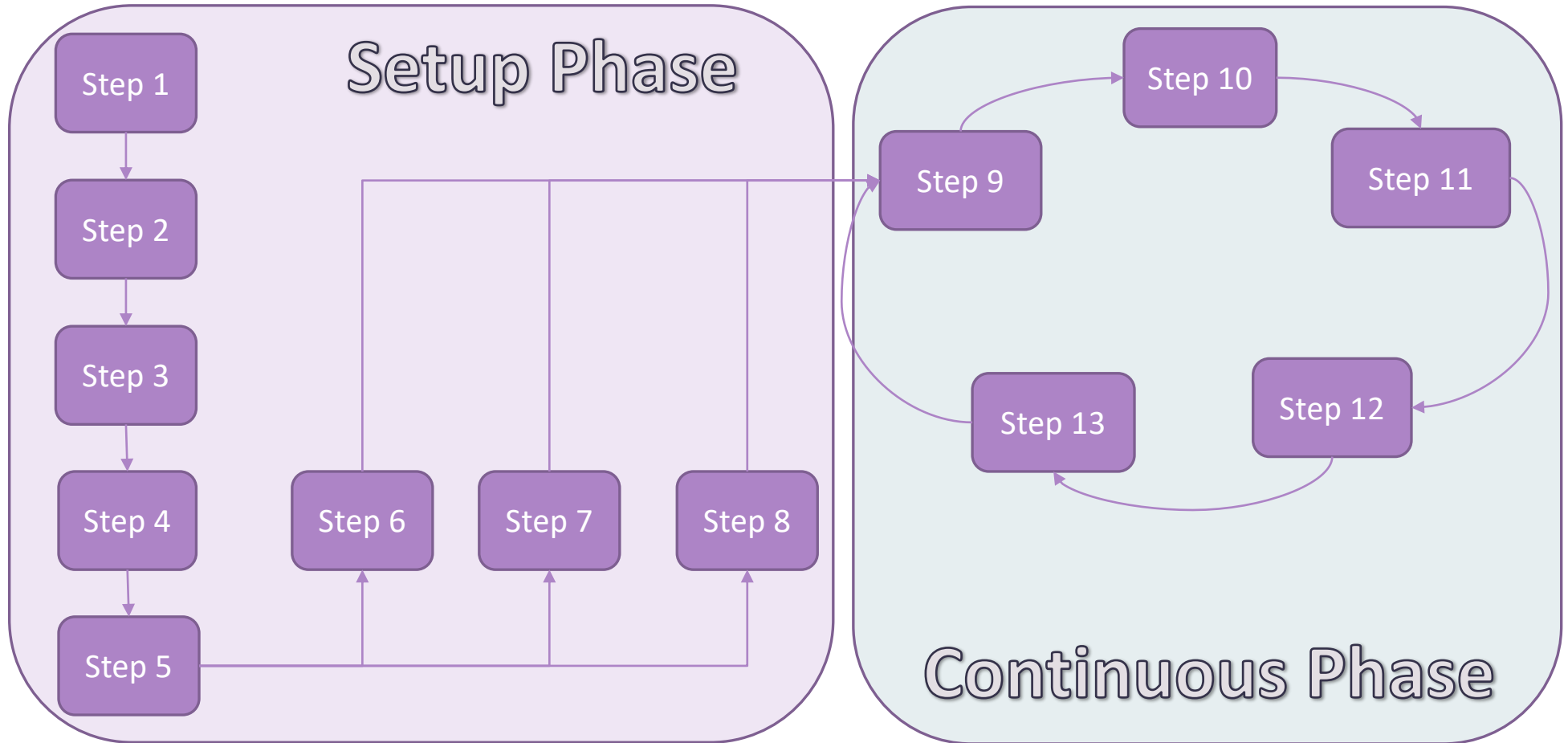
It is a complete methodology as it assumes that no ISG environment exists at all, and that everything must be started from scratch

In many companies the reality is much better

- re-use as much as possible to prevent wasting unnecessary time and money

The actual situation must be compared with the steps provided in the methodology, and must be synchronized and integrated where possible

Methodology Flow



Step 1

Get the Board's buy-in about IT Risk Management and Information Protection

- This is a very important starting point and without it, the project will surely have problems in progressing properly
- Initially it may not be possible to get a “clean” Board Directive but that is not essential
- As long as there is a commitment from the Board to support the project, that is enough to start
- The formal Board Directive can come later – but be sure to get it!

Step 2

Select some guiding Best Practices

- It is fundamental to choose some existing international Best Practice to use as a foundation for the project, and to provide motivation and direction
- Many Best Practice exists and the essential aspect is to have one

Step 3

Perform a basic Risk Analysis and determine all controls needed

- It is important to perform some type of Risk Analysis
- This is mandatory to identify actual critical assets and avoid wasting of money and investment
- Risk Analysis requires to get a wide spectrum of people involved
 - Board members, line management, users, system owners etc.
- Ensure that the relevant controls are installed and operational

Step 4

Create a Corporate Information Security Policy (CISP) and get it signed by the Chairman/CEO

- A CISP must be drafted, be circulated amongst the stakeholders and then submitted to top management.
- Recall: It is essential to have a more formal Board Directive on Information Security in order to write down a consistent CISP
- The Draft CISP must now be signed and made official company policy
- This is the basis and motivation for all future steps

Step 5

Create the rest of the Information Security Policy Architecture (ISPA)

- Documents composing the ISPA must be defined
- This can be done taking as input
 - the risk analysis conducted in Step 3
 - The CISP produced in Step 4
- ISPA documents can be defined by following the guidelines discussed in the previous lectures

Step 6

Create the organizational structure for ISG

- Specific attention must be given to the Operational Management and Compliance Management sides
- This step is closely related to Step 7 and this is why it is preferable to do them in parallel

Step 7

Create an initial set of Compliance/Control measures and start using these measures to create reports on all three management levels

- In this step, it is important to get buy-in from the company's Internal and External IT Auditor departments as well as the Legal department
- If these were involved in Step 3 above, this process will be much easier
- Recall: creating such measures is not straightforward, and the effectiveness and value of such measures will have to be refined over time
- It is, however, important to start off with an initial set of measures which will form the basis of the 'Control' part of the model

Step 8

Create an Awareness Programme including aspects like information security job responsibilities

- This step is core to the success of the whole effort and must be performed on a continuous basis
- All the documents in the ISPA should form part of the Awareness Programme

Step 9

Get the cycle going – kick start the process

- At this point, the whole programme must be initiated
- If one already exists, the revised one must be integrated with the existing one to get the new one operational.

Step 10

Redo the Risk Analysis from time to time to identify the possible changes in risks and controls

Risks are dynamic

- old ones go away (e.g., patches installed, port closed, access control mechanisms deployed)
- new ones materialize (e.g., new software installed, changes in the configuration parameters)
- existing ones change their impact (e.g., a single mitigation action may decrease the impact of all the other threats)

It is, therefore, important to redo any Risk Analysis from time to time to ensure that the risk situation is up to date and that relevant controls are installed and operational.

Step 11

Keep the ISPA up to date and in line with newly identified risks

- Ensure that all changed risks are reflected in the ISPA by changing the content of the ISPA and Compliance Clauses, if necessary.

Step 12

Refine and expand the Compliance Control measures to cater for newly identified risks, enforce compliance and keep reporting to top management

- Recall: The choice and creation of Compliance Clauses and Compliance Monitoring measures are not easy, and remain a challenging process
- The process never stops
 - experience is continuously gathered
 - It can be used to refine measures and create new ones.

Step 13

Continue to make all users more Information Security Aware

- This process can never stop and must be enforced on a continuous basis.