ISO 27001
Information Security Management Systems (ISMS)

ISSA PHOENIX
January 8, 2013

SECURASTAR
INFORMATION SECURITY

AGENDA

1. What is Information Security?
2. What is ISO 27001?
3. Define the Scope
4. Risk Management

SECURASTAR INFORMATION SECURITY

What is Information Security?

Question:

What is the most important asset in your organization?

INFORMATION

What is Information?

Information is an "Asset", that like any other important business asset, that has a critical value to the organization and thus needs to be adequately protected.

Information can exist in "ANY" form:

- **Electronic** – email, data stored, websites, etc.
- **Physical** – paper files, cd, photos, USB drive, etc.
- **Verbal** – phone conversations, in-person conversations, meetings, **Knowledge –** employee knowledge (in their heads)
- **Other?**

1 What is Information Security?

Information has 3 main attributes:

- ✓ **Confidentiality**
  The property that information is not made available or disclosed to unauthorized individuals, entities, or processes
- ✓ **Integrity**
  The property of safeguarding the accuracy and completeness of assets
- ✓ **Availability**
  The property of being accessible and usable upon demand by an authorized entity

**The importance of each component varies from organization to organization!*

SECURASTAR INFORMATION SECURITY

How do we define Information Security?

"The preservation of confidentiality, integrity and availability (CIA) of information in any form."

In addition, other properties such as authenticity, accountability, non-repudiation and reliability may also be involved.

[ISO/IEC 27002:2005]

Information security management is a **management** process NOT a technical process!

It's all about **managing**

- People
- Processes
- Assets
- Risks
- ...

From an information security management perspective, technology is a control (anti-vírus, firewalls, IPS, etc.) *we put in place to mitigate risk, ...not the opposite!*

Practicing information security is often an unorganized, reactive and a bottom up approach.

Practicing Information Security (Reactive)**:**

- No Management Commitment
- No information asset inventory
- No risk assessment
- No way to evaluate or prioritize risk
- No way to evaluate if controls are adequate
- No metrics
- No improvement
- Compliance???

Managing information security is an organized, proactive and top down process approach!

Managing Information Security (Proactive):

- Requires Management Commitment
- Defined Scope and boundaries of the ISMS
- Information asset inventory
- Risk assessment
- Selection of controls based on risk / Prioritization
- Metrics to monitor control maturity
- Continuous improvement cycle
- Measured Compliance
- Reasonable Assurance to Interested Parties (stakeholders)

What is ISO 27001?

Management Systems

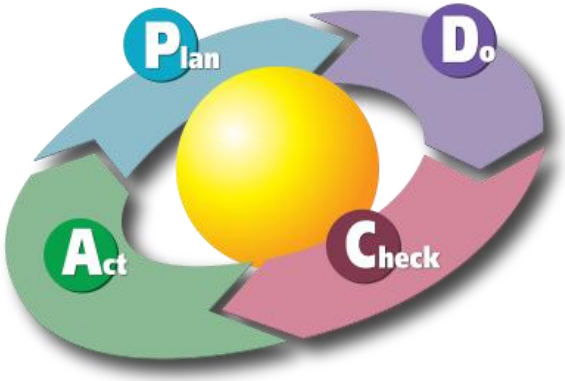
"A **management system** is the framework of processes and procedures used to ensure that an organization can fulfill all tasks required to achieve its objectives."

ISO Guide 72

- ISO 9001 – Quality Management System (QMS)
- ISO 14001 – Environmental Management System (EMS)
- ISO 20000 – IT Services Management System (ITSMS)
- **ISO 27001 – Information Security Management System (ISMS)**
- ISO 22301 – Business Continuity Management System (BCMS)
- ISO 22000 – Food Safety Management System
- OHSAS 18001 – Health & Safety Management System
- *Others*

PDCA model (Dr. W. Edwards Deming)

All ISO management systems are based on the PDCA continuous improvement cycle methodology



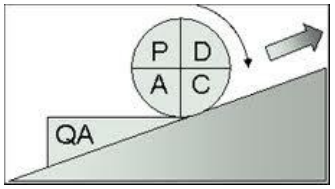
PLAN – Establish, assess, define

DO – Implement, operate, produce

CHECK – Audit, measure, monitoring

ACT – Improve, correct, prevent

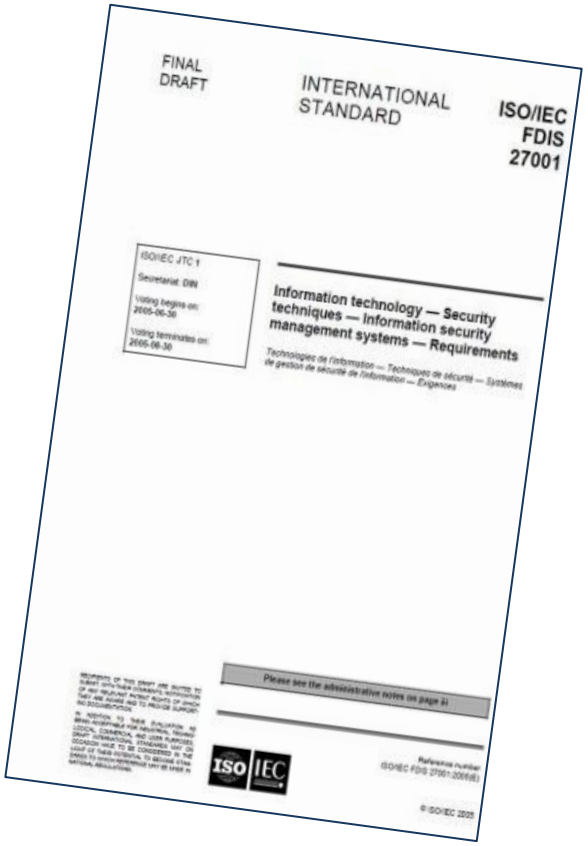
Key concept *– Continuous improvement =*



2 What is ISO 27001?

ISO 27001 is a standard (set of requirements) to establish, implement, operate, monitor, review, maintain and improve a documented Information Security Management System (ISMS) within the context of the organization's **Risk** to its Information Assets (information in "Any" form)**.**

The **ISMS** is designed to ensure the selection of adequate and proportionate security controls, that protect information assets and give confidence to interested parties (reasonable assurance).


FINAL DRAFT

INTERNATIONAL STANDARD

ISO/IEC FDIS 27001

ISO/IEC JTC 1

Secretariat: DIN

Voting begins on: 2005-06-30

Voting terminates on: 2005-08-30

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences

Please see the administrative notes on page iii

ISO IEC

Section 4-8
Auditable Requirements

Quality based management requirements (auditable) that "shall" be met by an Information Security Management System (ISMS) used to manage the information security program.

SECTION 4	Information Security Management System (ISMS)
4.1	General Requirements
4.2	Establishing and Managing the ISMS
4.2.1	Establish the ISMS = **PLAN**
4.2.2	Implement and Operate the ISMS = DO
4.2.3	Monitor and Review the ISMS = CHECK
4.2.4	Maintain and Improve the ISMS = ACT
4.3	Documentation Requirements
4.3.1	General
4.3.2	Control of Documents
4.3.3	Control of Records
SECTION 5	Management Responsibility
5.1	Management Commitment
5.2	Resource Management
5.2.1	Provision of Resources
5.2.2	Training, Awareness and Competence
SECTION 6	Internal ISMS Audits
SECTION 7	Management Review of the ISMS
7.1	General
7.2	Review Input
7.3	Review Output
SECTION 8	ISMS Improvement
8.1	Continual Improvement
8.2	Corrective Action
8.3	Preventive Action

Annex A – 11 Control Objectives / 133 Controls

A comprehensive minimum baseline of information security controls that all information security programs must consider when selecting controls to mitigate risks (Risk Management).

#	Ref	Description
1	A5	Security policy
2	A6	Organization of information security
3	A7	Asset management
4	A8	Human resources security
5	A9	Physical and environmental security
6	A10	Communications & operations management
7	A11	Access control
8	A12	Information systems acquisition, development & maintenance
9	A13	Information security incident management
10	A14	Business continuity management
11	A15	Compliance

*"The requirements in ISO 27001 auditable sections 4-8 are **generic** and are intended to be applicable to all organizations, regardless of type, size and nature."*

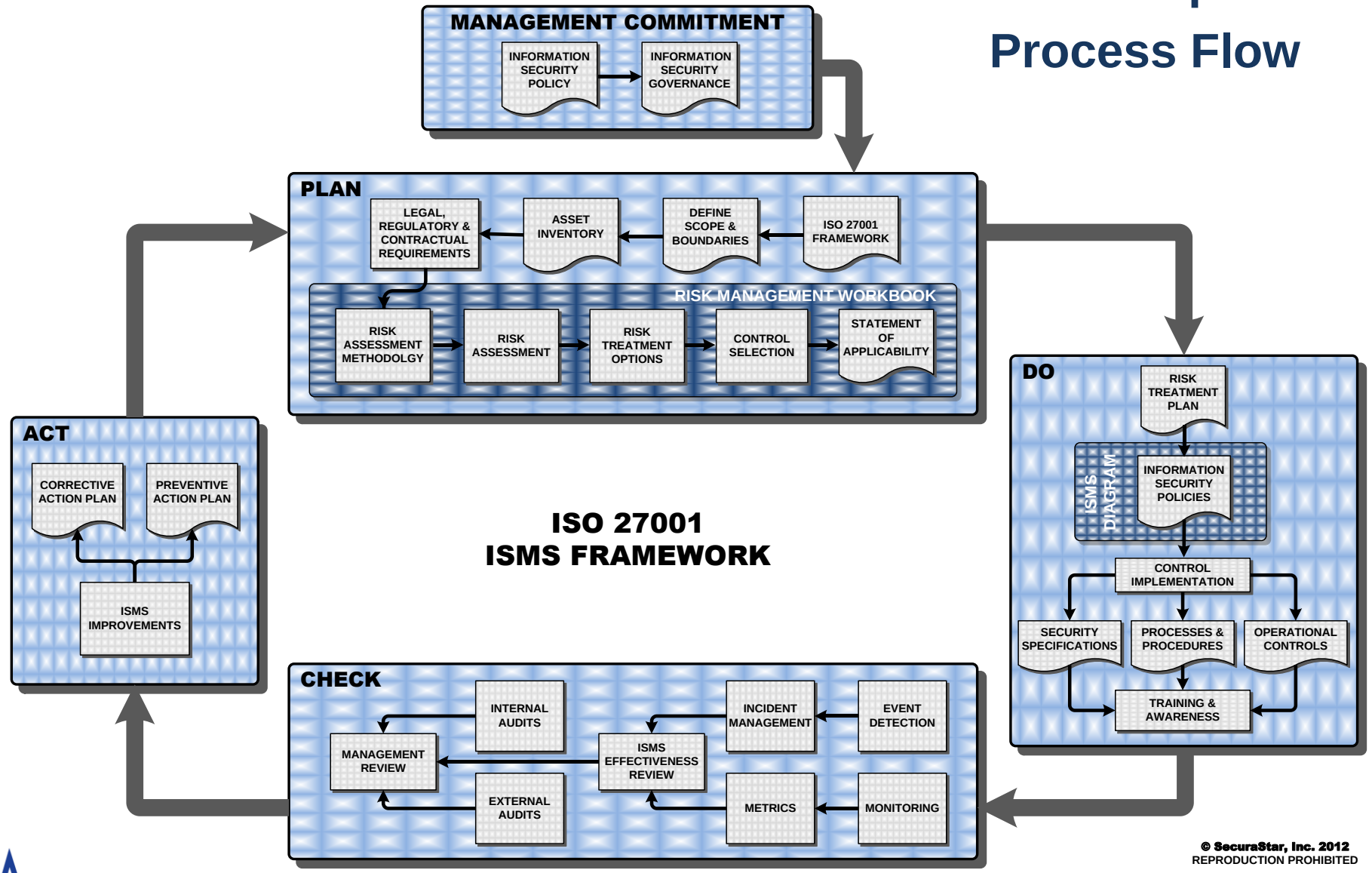
GENERIC REQUIREMENTS?.....

Then how do you implement ISO 27001?

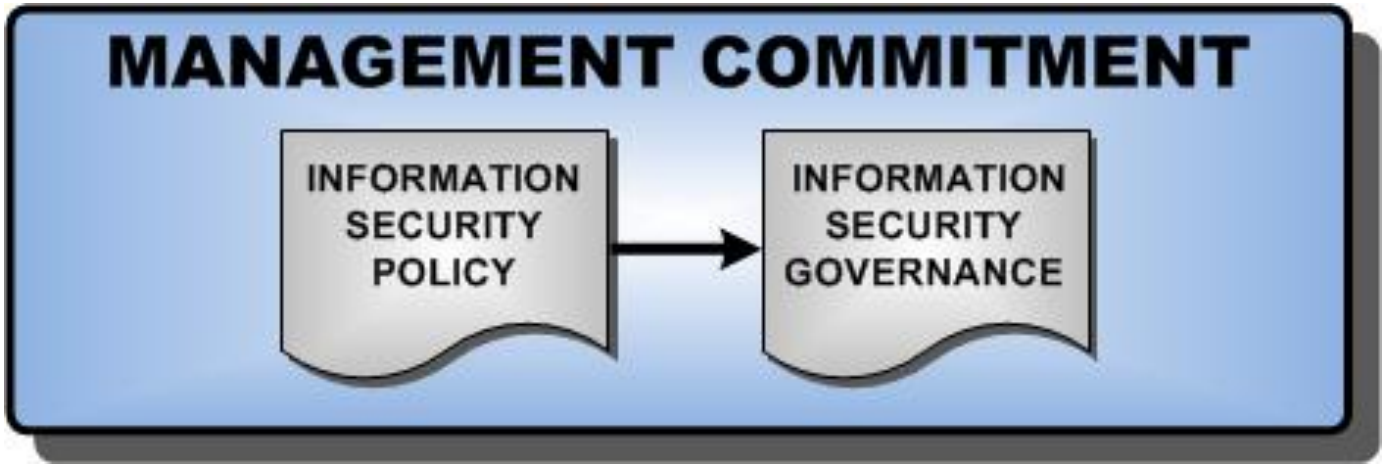
&

What does ISO 27001 Framework look like?

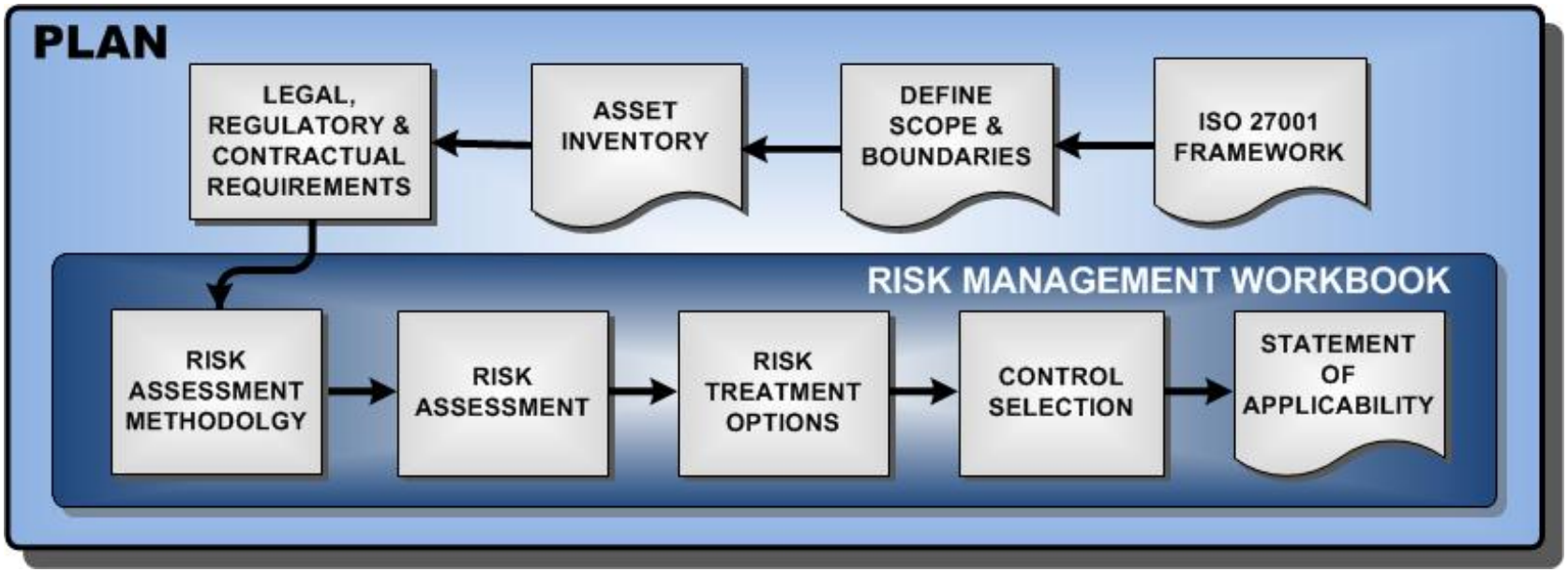
5 Step Process Flow



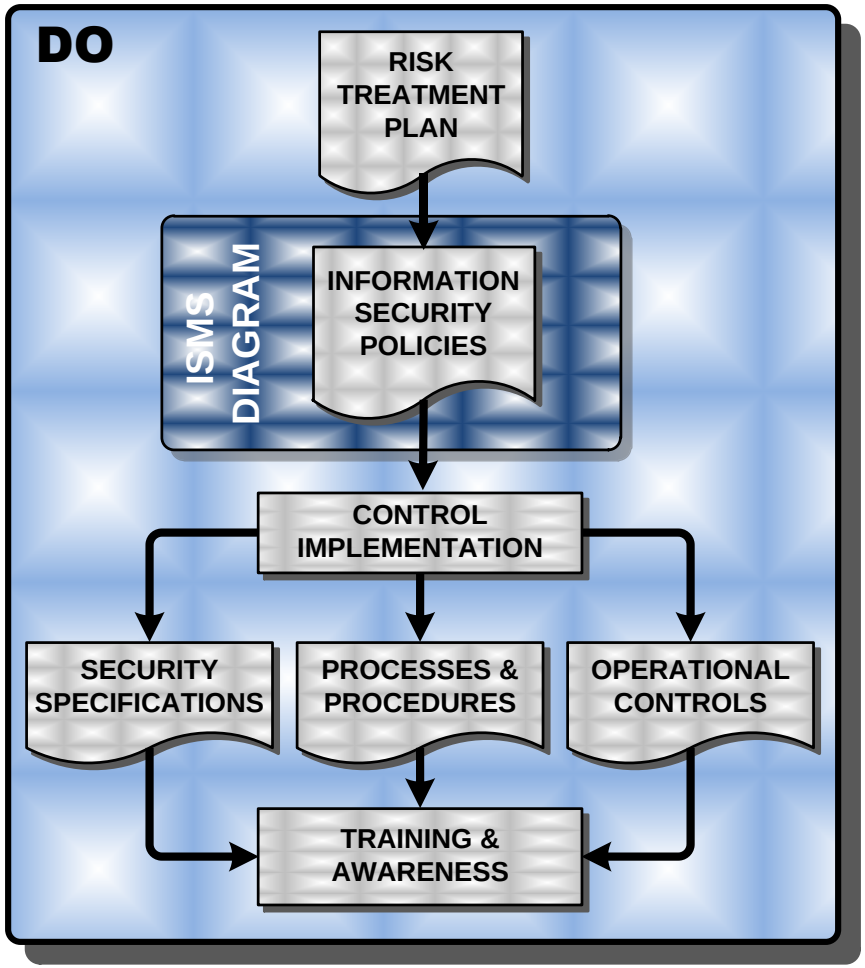
1. Obtain Management Commitment



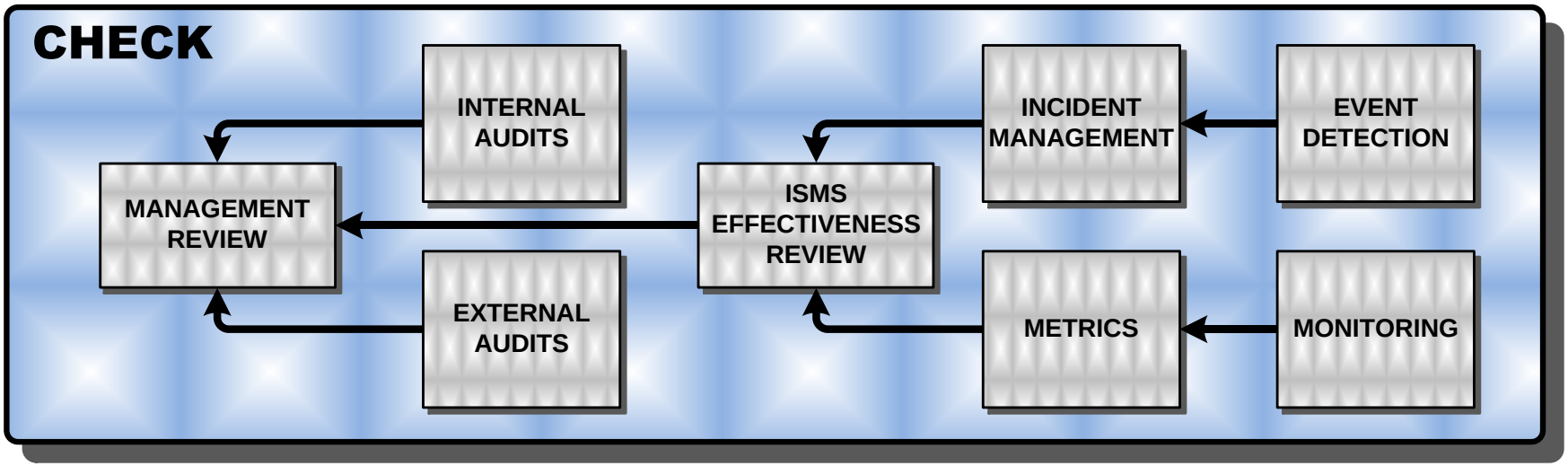
2. Establish the ISMS = PLAN



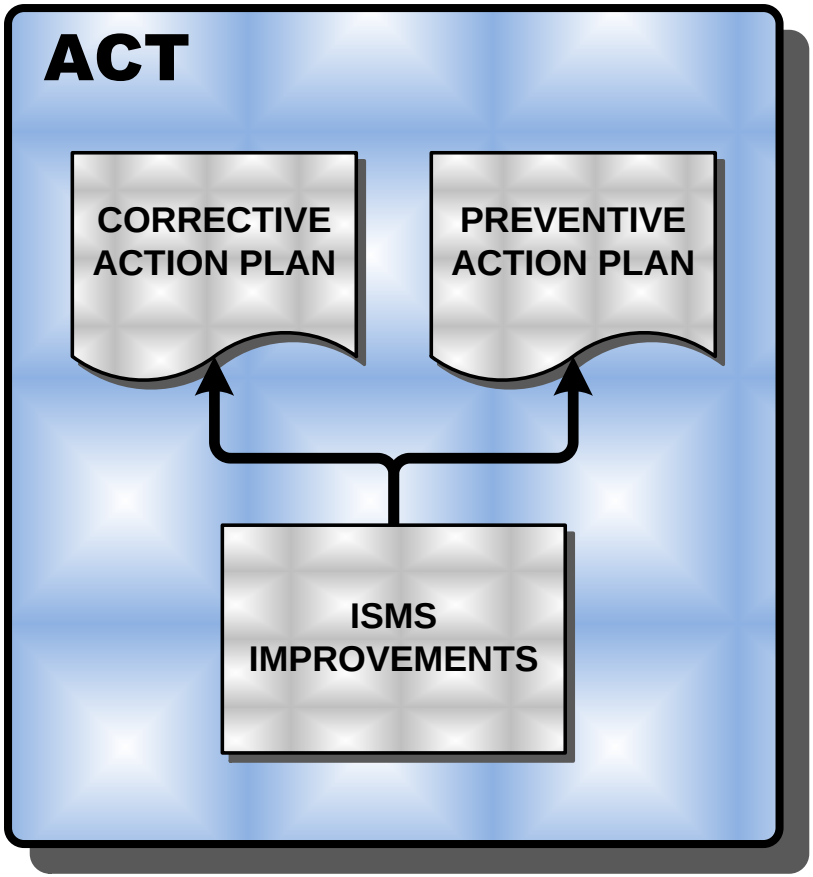
3. Implement & Operate the ISMS = DO



4. Monitor and Review the ISMS = CHECK



5. Maintain and Improve the ISMS = ACT



PLAN
Define the Scope

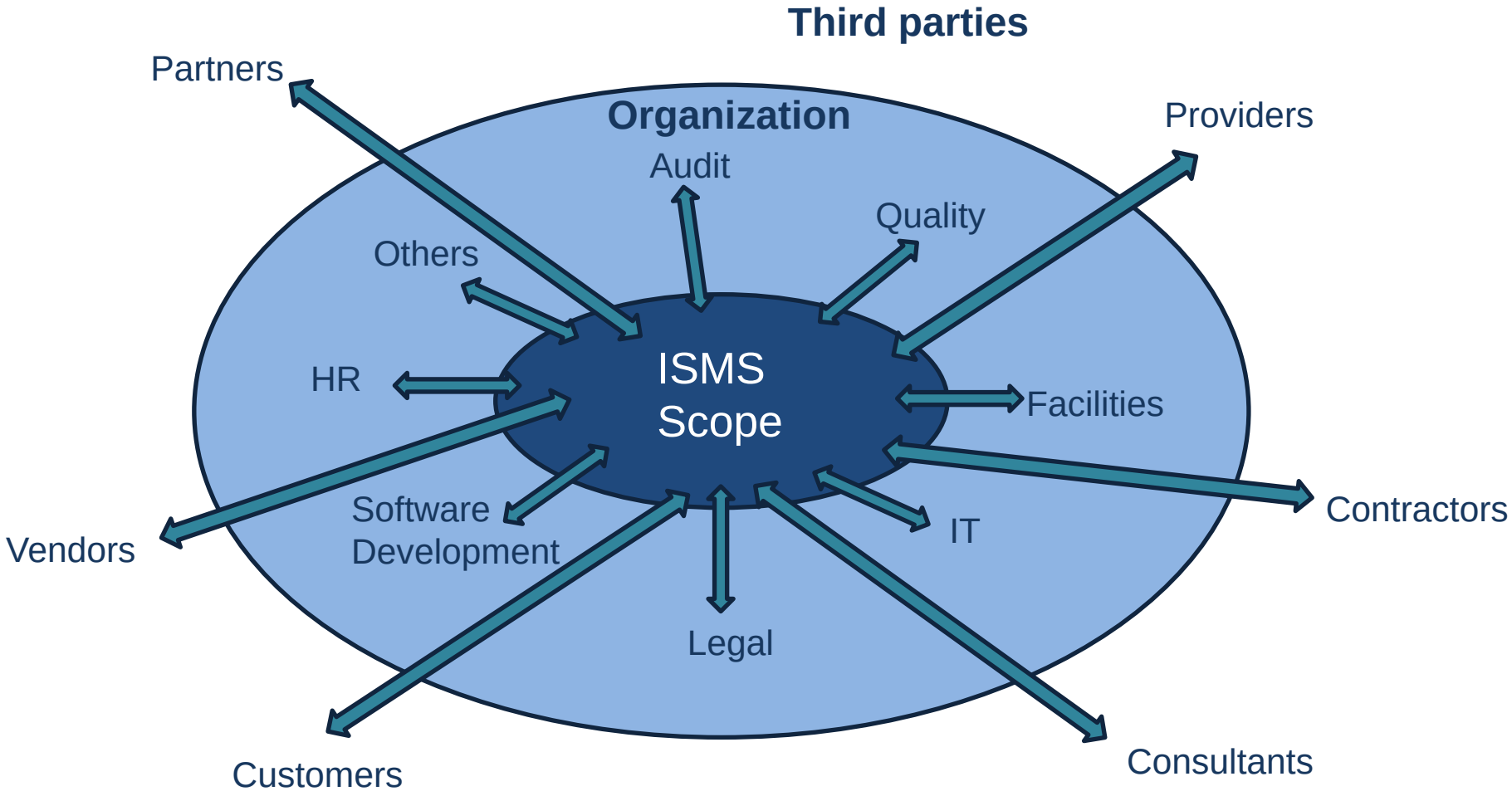
Define the Scope & boundaries

- The scope definition is the most important step in the whole process.
- The scope will have a huge impact on the rest of the implementation project, including costs and effort.
- It should meet business requirements and add value to products and/or services.
- So make sure you choose carefully!

The SCOPE is always a business decision!!!

Define the Scope & boundaries

Along with the scope one must define its boundaries, i.e. third parties and respective connections



Scope and Boundaries of the ISMS

Describe what is In Scope:

The <Organization> ISMS scope of registration includes all systems, networks, facilities and personnel that support the <Business Process>.

Describe what is not in Scope:

The <Organization> ISMS scope of registration does not include any systems, networks, facilities and people that support any other remaining business processes within <Organization>.

Now we can create an Information Asset Inventory

Define all information related assets within the Scope including:

- Information
- People
- Facilities
- Hardware / software / applications
- Other assets?

Asset Inventory (within scope)

Type	Category	Asset	Owner	Location	Processes
Hardware	Servers	Web servers	Manager	Los Angeles DC / Frankfurt DC	P1
		Application servers			
		File share/backups servers			
		Database servers			
	Desktops	22 desktops	Employees	Headquarters; Frankfurt office	P1, P2
	Laptops	22 laptops			
	Mobile computings (tablets, smartphones, etc.)	22 smartphones; 2 tablets (Name and Name)			
	Printers/copiers	Office printers	Manager	Headquarters	

PLAN
Risk Management

The Risk Management Process

Methodology

- Any methodology can be used;
- Shall ensure that risk assessments produce comparable and reproducible results;
- It must be used in all risk assessment processes within the organization (scope);
- Usage of software tools it s optional

Risk Assessment process

Risk = Impact x Likelihood

- **Impact**
  The consequences to the organization that a certain situation occurs
  - ✓ Financial impact
  - ✓ Image/credibility impact
  - ✓ Legal/Regulatory impact
  - ✓ Other impacts to the organization according to business requirements
- **Likelihood**
  The existing probability of a threat to explore a certain vulnerability
  - ✓ Threat
  - ✓ Vulnerability

Example of Impact & Likelihood Scales

IMPACT	DESCRIPTION
1	The harm to the Organization is **VERY LOW**
2	The harm to the Organization is **LOW**
3	The harm to the Organization is **MEDIUM**
4	The harm to the Organization is **HIGH**
5	The harm to the Organization is **CRITICAL**

LIKELIHOOD	DESCRIPTION
1	The probability of such event is **VERY LOW**
2	The probability of such event is **LOW**
3	The probability of such event is **MEDIUM**
4	The probability of such event is **HIGH**
5	The probability of such event is **CRITICAL**

EXAMPLE: Risk Assessment Matrix based on 1-5 impact and likelihood scales.

Sample: *"This organization accepts current risks rated less than or equal to **5** on the impact and likelihood risk matrix"*

CATEGORY	RANGE
LOW RISK	<=5
MEDIUM RISK	>5 <20
HIGH RISK	=> 20

RISK	LIKELIHOOD				
IMPACT	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Risk Treatment Options

There are 4 options for risk treatment:

- **Acceptance**
  - Accept the risk based on business decision
- **Mitigation**
  - Select the controls to mitigate the risk
- **Transfer**
  - Outsource a process
  - Insurance Policy
- **Terminate**
  - Terminate the process

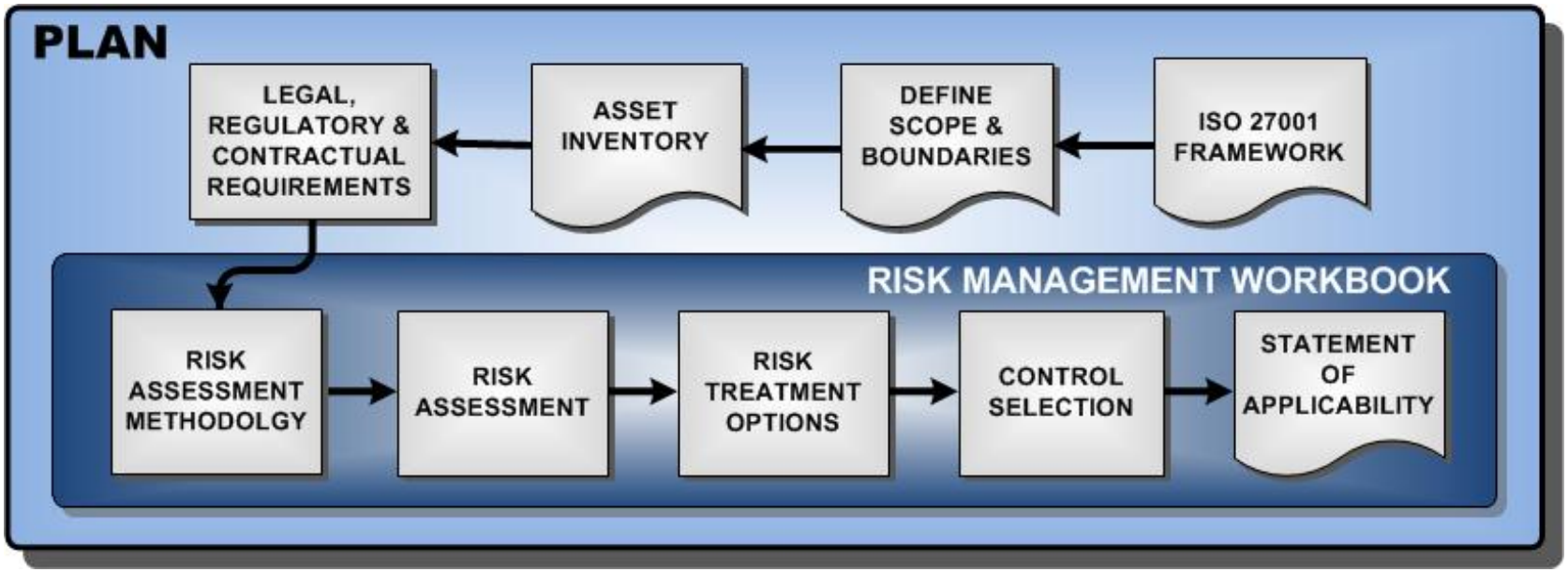
Control Selection

- Select control objectives and controls for the treatment of risks (Annex A – 133 Controls).
- Control objectives and controls shall be selected and implemented to meet the requirements identified by the risk assessment and risk treatment process.
- This selection shall take account of the criteria for accepting risks (see 4.2.1c)) as well as legal, regulatory and contractual requirements.

Risk Treatment Plan (RTP)

- One of the required documents in ISO 27001
- Output from the Risk Assessment
- The RTP is the Control Implementation Project Plan
  - Control to implement
  - Objective/s to achieve
  - Responsible for the task
  - Resources
  - Dates (planned, real)
  - Status

2. Establish the ISMS = PLAN



THANK YOU!

www.SecuraStar.com

Paulo Porfirio
Managing Partner Europe
Director of Service Delivery
Direct 651-253-3612
Paulo.Porfirio@SecuraStar.com

Dave Anders
CEO
Managing Partner (Worldwide)
Direct 612-703-1903
djanders@SecuraStar.com

SECURASTAR INFORMATION SECURITY