SECMAN

## SECMAN

### General marking

=> Devide the marks into the amount of things it's asking for. If it's asking for multiple things then you should answer in multiple things.

##### Focus:

on the how :  
=> understanding how security solutions control risk, bring down risk.  
the ability to communicate and articulate what a control proposed to bring down risk is vital.

##### Week 1 (Nov 22)

Information Security:  
Protection of the **confidentiality**, **integrity** and **availibility** of **information** assets, whether in **storage**, **processing** ir **transmission** via the application of **policy**, **SETA\*** and **technology**

**Information Security Management Systems - ISO 27000**  
Organizations of all types and sizes:

* collect, **process**, **store**, and **transmit** information
* recognize that **information**, and related **processes**, **systems**,  
  **networks** and **people** are important assets for achieving  
  organization objectives.
* face a range of **risks** that may **affect** functioning of **assets**
* address their perceived risk exposure by implementing  
  information **security controls**  
  Coordinated activities directing the implementation of suitable  
  controls and treating unacceptable information security risks are  
  generally known as elements of **information security**  
  **management.**

#### What is an ISMS?

**Information Security Management Systems - ISO 27000**  
As information security risks and the effectiveness of controls  
change depending on shifting circumstances, organizations need to:  
• **monitor** and **evaluate** the effectiveness of implemented  
controls and procedures  
• **identify** emerging risks to be treated  
• **select**, **implement** and **improve** appropriate controls as  
needed.  
To interrelate and coordinate such **information security** activities,  
each organization needs to establish its policy and objectives for  
information security and achieve those objectives effectively by  
using a **management system.**

#### ISMS Frameworks

There are a number of Risk Management Frameworks  
• ISACA COBIT  
• ISO/IEC 27005  
• NIST 800-30  
Equally, there are a number of ISMS Frameworks:  
• ISACA COBIT  
• ISO/IEC 27000 series  
• NIST CSF

##### More info : [Link](https://www.ncsc.gov.uk/collection/risk-management-collection/component-system-driven-approaches)

#### ISO/IEC 27001

* ISO/IEC 27000 provides an overview of information security management  
  systems and defines related terms.
* ISO/IEC 27001 specifies requirements for an ISMS
* An ISMS is an information assurance framework adopted to establish,  
  implement, operate, monitor, review, maintain and improve information  
  security
* It specifies a Plan-Do-Check-Act cycle:
  + **Plan**: Establish the ISMS
  + **Do**: Implement and Operate the ISMS
  + **Check**: Monitor and Review the ISMS
  + **Act**: Maintain and Improve the ISMS
  + While it specifies the “what needs to be done”,  
    it’s short on “how to do it”
* ISO/IEC 27001 is seen as more flexible even than NIST CFS (It doesnt describe the how to do it, hence, more freedom)
* ISO/IEC 27001 is a certifiable framework of how to establish an ISMS
* ISO/IEC 27002 is the necessary controls and implementation guidance.

*More used since its less specific or concrete in describing what needs to be done*

#### ISO/IEC 27002

ISO/IEC 27002 makes recommendations to those responsible for initiating, implementing or maintaining security in an organisation  
It specifies/outlines a number of controls across:

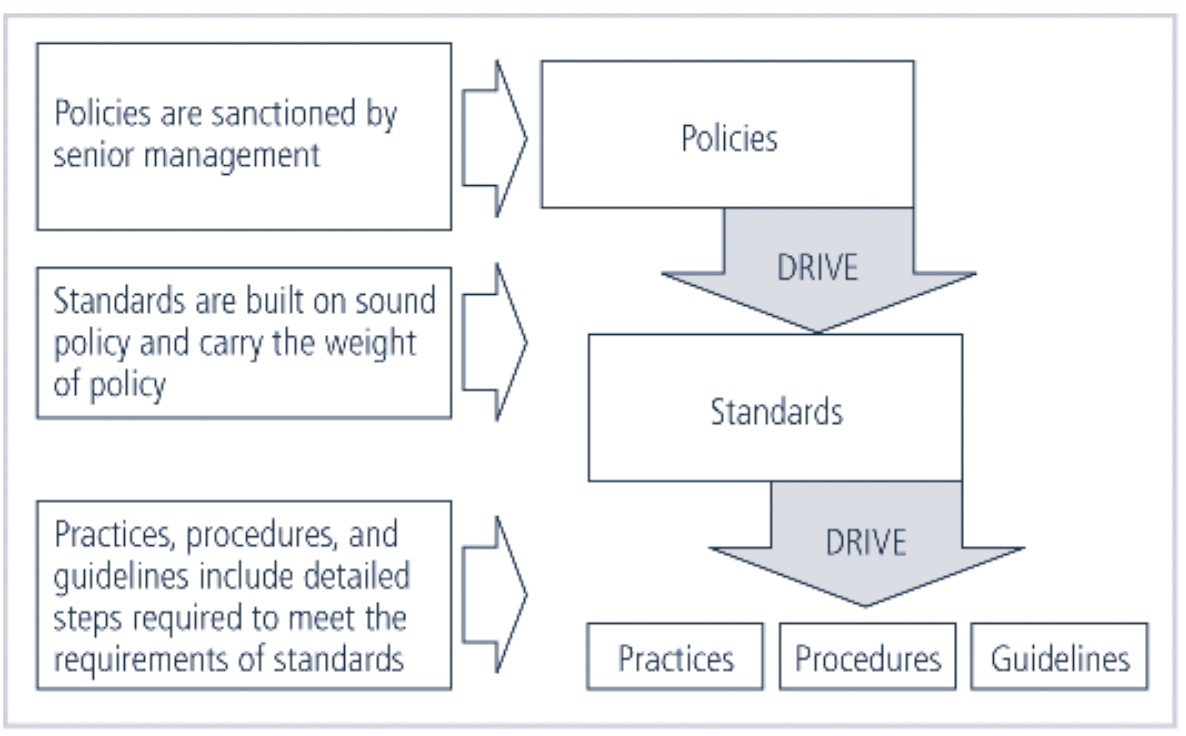
-tx-  
| ISO/IEC 27002||  
-|-  
Security Policy |Organisation of Info Security  
HR Security |Asset Management  
Access Control |Cryptography  
Physical/Env. Security|Operations Security  
Comms Security |IS Acquisition  
Supplier Relationships |Incident Management  
Business Continuity |Compliance

#### Policies, Standards, Guidelines and Procedures

* Policy A principle or rule to guide decisions and achieve  
  rational outcomes  
  *Implies that policies can't be completetly specified. It provides principles to be followed*
* Standards Detailed statements, quantifying what must be  
  done to comply with policy  
  *Are additional information to support Policy. Making detailed staments that contify what must be done to comply with Policy*
* Guideline A set of recommended actions to assist in  
  complying with policy  
  *Dont nessearily need to be followed but give ways in order for employees to comply with Policies. You still have to follow the standards provided*
* Procedure A list of steps that constitute instructions for  
  performing some action or accomplishing some task  
  *An exact set of steps to be followed*

##### TL;DR

*policy is the most important document, the rest are just to support it*  
**Policy** is what we want => **Standard** is strict rules to acheive the **policy** => **Guidelines** are a "guide" to help fall in line with the **policy**, hence, also falling in line with **Standards**



##### Importance of policies ISM

-tx-  
|Policy documents should help to:||  
--|--  
|Identify assets the company considers valuable ||  
|Provide authority to the security team and its activities ||  
|Provide a reference to review when conflicts pertaining to security arise ||  
|State the company’s goals and objectives pertaining to security ||  
|Outline personal responsibility ||  
|Help to prevent unaccounted-for events (surprises) ||  
|Define the scope and functions of the security team ||  
|Outline the company’s response to legal, regulatory, and standards of due care||  
|Outline incident response responsibilities||

* *if an employee is uncertain on what to do, they should be able to check the policy for guidance. This should be the first call of order*
* *Policies should definitely state the companies goals and objectives pertaining to information security. Not just specify the security has authority, but remid employee's have a resposibility.*
* *ISP help to account for events and surprises and define the scope and functions of the security team. This doesnt just give them authority but also outline the scope of their authority*
* *Policies not only help prevent security threats, but outline responsibilities in responce to security incidents if the worst should happen*

For policies to be effective, and organisation should be able to demonstrate:

* Dissemination (distribution)
  + in a way that makes it readily available for review by all employes that are expected to comply with that policy
* Review (reading)
  + needs to be accisible, intelligable. might be providing different versions for different languages etc...
* Comprehension (understanding)
  + demonstrate the employee understands the policy and their responsibilities. they comprehend each of the aspects of the policies. Maybe use a quiz to display understanding of the policies.
* Compliance (agreement)
  + need to make sure the emplyee agreed to follow and comply to the policy
* Uniform Enforcement
  + Demonstrate the policy is uniformly enforced regardless of status or assignment.