Teesside University

# Information Governance CIS3005

ISO 27K & information governance frameworks (1)

# Introduction

- A big area to look at this week – Information Security *Policy* in general and Information Security Management Systems (ISMS) more specifically
- Very important
  - Job market
  - Importance for organisations
  - Not everyone’s “cup of tea”, but you absolutely can’t ignore it!
- We will be looking at:
  - Policy at macro and micro level
  - ISO27K standard
    - Overview and
    - Some parts in more detail
- This lecture will contribute to LO’s 4 & 5

# Information Security (IS) Policy

- Information security Policy can be at a:
- Macro(national) level
  - National Cyber Security Strategy 2022-2030
- Micro (organisational) level
  - Teesside Uni – a number of different docs:
    - Legal Regs
    - Computer Regs
  - NHS England Information Security Policy
- ALL organisations will have a series of documents like these. The documents state in writing how an organisation plans to protect the org's physical and IT assets
  - Not only does the company need to protect its IT & IP assets it also needs to comply with relevant legislation & regulations, address threats, establish a code of conduct
    - E.g. DPA 2018, GDPR, Protection from Harassment Act 1997, Copyright, Design and Patents Act 1988

# Importance of knowledge of standards

- If you Google the following job titles (Reed.co.uk is a good place to look), you will find in the past week:
  - Information/IT security analyst 254 jobs (173 as at March 2023).
    - Information Security Analyst
  - Information Governance 746 jobs
    - E.g. Information Governance Officer
  - What commonalities do you see?
  - Growth area and all want knowledge of legal issues and standards (ISO)

# Knowledge of standards

- Many roles and jobs require some knowledge of policies and standards
  - Information Governance jobs – this is essentially what they are about
- The standards they are most concerned about are:
  - BS 7799 (British standard published in 1995), this was adopted by international standards bodies as:
  - ISO 17799 “Code of Practice for information security management” in 2000.
  - Then incorporated into **ISO 27000 series** in 2007
  - BS 7799-2 (1999) focussed on how to implement an **Information Security Management System (ISMS)** **– this later became ISO 27001** in 2005

# How do you create a good Information Security Policy for an organisation?

- Copy what someone else has done
  - Many organisations publish their IS Policy to some extent
  - What are the problems with this approach?
- Buy a policy or system from one of the many companies offering this service (E.g.)
  - What are the potential problems with this approach?
- "Have a go" at doing it in-house
  - What are the potential problems with this approach?
  - What are the benefits?
  - What resources are needed?
- How to create a good information security policy
- Increasingly orgs look to a set framework or standard to help give structure to a ISMS
  - Now very difficult to get contracts *without* a standard compliant ISMS in place
- Increasingly the standard people look to is the ISO 27K standard
  - ITIL & Cobit also useful (more on these next week)

# So what is ISO27k?

- Internationally recognised **STANDARD** developed by the International Organisation for Standardisation
- Actually a family of interlinked standards that “provides best practice recommendations on information security management - the management of information risks through information security controls - within the context of an overall Information security management system (ISMS)”
- From the ISO website:
- “The ISO/IEC 27000 family of standards helps organizations keep information assets secure. Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties”.
- What is an ISMS?
  - An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.
  - It can help small, medium and large businesses in any sector keep information assets secure.”
  - The cost of ISO 27K certification varies depending on factors such as the size and complexity of your organisation, the number of locations, and the technology used

# So what is the “ISO 27000 series”?

- ISO 27000 – Provides an overview of the standard & vocabulary
- **ISO27001 – Specifies the Requirements of an ISMS**
  - **Contains Annex A – Information Security Control Reference**
- **ISO 27002 – Code of Practice for IS controls that are listed in Annex A.**
  - “is a popular international standard describing a generic selection of ‘good practice’ information security controls, typically used to mitigate unacceptable risks to the confidentiality, integrity and availability of information.”
- **ISO 27003 – ISMS implementation guidance**
- ISO 27004 - Information security management – Monitoring, measurement, analysis and evaluation.
- **ISO 27005** - **Information security risk management.**
- ISO 27006 - Requirements for bodies providing audit and certification of information security management systems.
- ISO 270035 - concern managing information security events, incidents and vulnerabilities, expanding on the information security incident management section of ISO/IEC 27002.

## ISO 27002:2022 - Information security, cybersecurity and privacy protection — **Information security controls** *(3rd ed)*

“*This document is designed for organisations of all types and sizes. It is to be used as a reference for determining and implementing controls for information security risk treatment in an information security management system [ISMS] based on ISO 27001*”

The standard is explicitly concerned with *information* security, meaning the security of all forms of information (*e.g.* computer data, documentation, knowledge and intellectual property) and not just IT/systems/network/cyber security.

Standard lays out 93 info sec controls based around 4 “themes”

5. Organisational (37 controls)
6. People (8 controls)
7. Physical controls (14 controls)
8. Technological controls (34 controls)

- *Controls* are policies (things that need to be done and checked) defined, approved by management, published to employees & external parties. These should be reviewed and revised at regular intervals.

# 4.2: Attributes (see 27002 s4.2 for more explanation)

5 attributes can be applied to each control to better suit the needs of an organisation:

a) Control types
   i. Preventative (prevents the occurrence of an info sec incident)
   ii. Detective (control acts when an info sec incident occurs)
   iii. Corrective (control acts after an info sec incident occurs)

b) Information security properties
   i. Which characteristic of information the control will contribute to preserving: **c**onfidentiality, **i**ntegrity & **a**vailability

c) Cybersecurity concepts
   i. Linked to ISO 27110
   ii. Values consist of: Identify, Protect, Detect, Respond & Recover

# 4.2: “Attributes” (Annex A of standard)

d) Operational capabilities

   i. Practitioner’s perspective of info sec capabilities, can include – governance, asset management, human resource security, identity & access management, continuity, legal & compliance etc

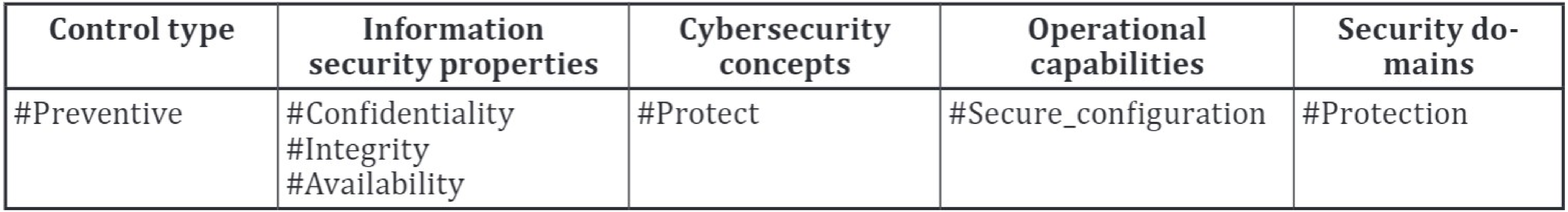
e) Security domains

   i. To view controls from perspective of 4 info sec “domains”

      1. Governance & Ecosystem (incs info sys security, governance & risk management etc)
      2. Protection (incs IT security architecture, IT security admin, identity & access management etc)
      3. Defence (incs detection & computer security incident management)
      4. Resilience (incs continuity of operations & crisis management)

# Example of actual control within a section

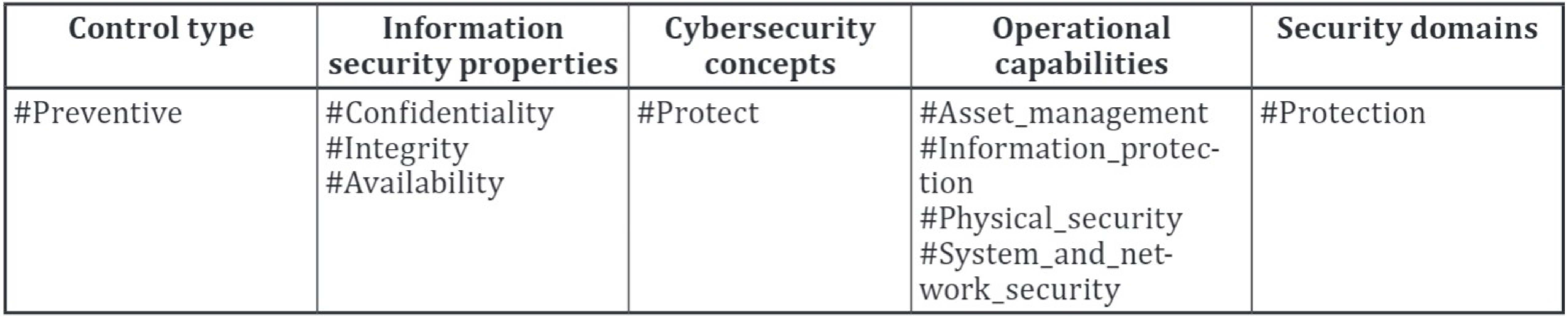
- **8.24: Use of Cryptography**
  - Control = Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.



| Control type | Information security properties | Cybersecurity concepts | Operational capabilities | Security domains |
|---|---|---|---|---|
| #Preventive | #Confidentiality<br>#Integrity<br>#Availability | #Protect | #Secure_configuration | #Protection |

# Example 2 – **6.7: Remote working**

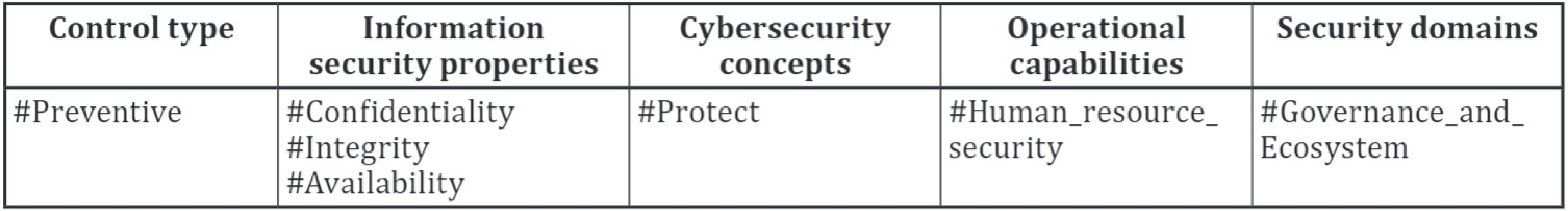
Control = “Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization’s premises”



| Control type | Information security properties | Cybersecurity concepts | Operational capabilities | Security domains |
|---|---|---|---|---|
| #Preventive | #Confidentiality<br>#Integrity<br>#Availability | #Protect | #Asset_management<br>#Information_protection<br>#Physical_security<br>#System_and_network_security | #Protection |

# Example 3 - **6.3: Information security awareness, education and training**

Control = “Personnel of the organisation and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization’s information security policy, topic-specific policies and procedures, as relevant for their job function”



| Control type | Information security properties | Cybersecurity concepts | Operational capabilities | Security domains |
|---|---|---|---|---|
| #Preventive | #Confidentiality<br>#Integrity<br>#Availability | #Protect | #Human_resource_security | #Governance_and_Ecosystem |

# ISO 27003 – Security techniques – ISMS Guidance

- Provides guidance on implementing ISO27002
- Linked to specification described in ISO27001
- Provides;
  - Recommendations (should)
  - Possibilities (can)
  - Permissions (may)
- E.g. **section 7.3: Awareness**
  - **Required activity**: The persons doing work under the organisation’s control are made aware of the information security policy, their contribution to the effectiveness of the ISMS, benefits of improved information security performance and implications of not conforming to the requirements of the ISMS
  - **Guidance - The organisation should**:
    - Prepare a programme with the specific messages focussed on each audience (external & internal people)
    - Include information security needs and expectations within awareness and training materials on other topics to place information security needs into relevant operational contexts
    - etc

# Conclusion

- There is an *awful* lot to think about this week
- The ISO27K set of standards isn't the easiest thing to get your head around, but before our next session please do look at the following:
  1. You can access the standards themselves via the library:
     - On the Library website select "Databases" > select the letter "B" > Scroll down to "British Standards Online" > in the search box enter "27002" (look for new 2022 standard) for example > select the standard you want to look at and either download the PDF or Select "Quick View"
       - **NB** You will **not** be able to find copies of these standards on the internet, you are expected to pay for them, but as a student you have free access to these very valuable resources!
  2. Also have a look at: https://www.iso27001security.com/index.html The site gives an overview of all the ISO27K standards and also provides a free Toolkit to help you prepare your business to go for ISO27K certification (more on this next week)
     - The site is built and maintained by a group of volunteers and whilst it looks a little basic it is very useful and informative.

# Conclusion

- We have:
  - Had an overview of the ISO27k
  - Looked at some of the different standards within the “family”
    - Concentrated on ISO27001, 27002 & 27003
  - Considered what is meant by “control objectives” and the “controls” that help achieve the objectives
- Next week we will be:
  - Looking at ISO27005 (Assessing Risk)
  - Certification and accreditation
  - Training levels
  - Importance to businesses
  - Look at alternatives – ITIL & COBIT