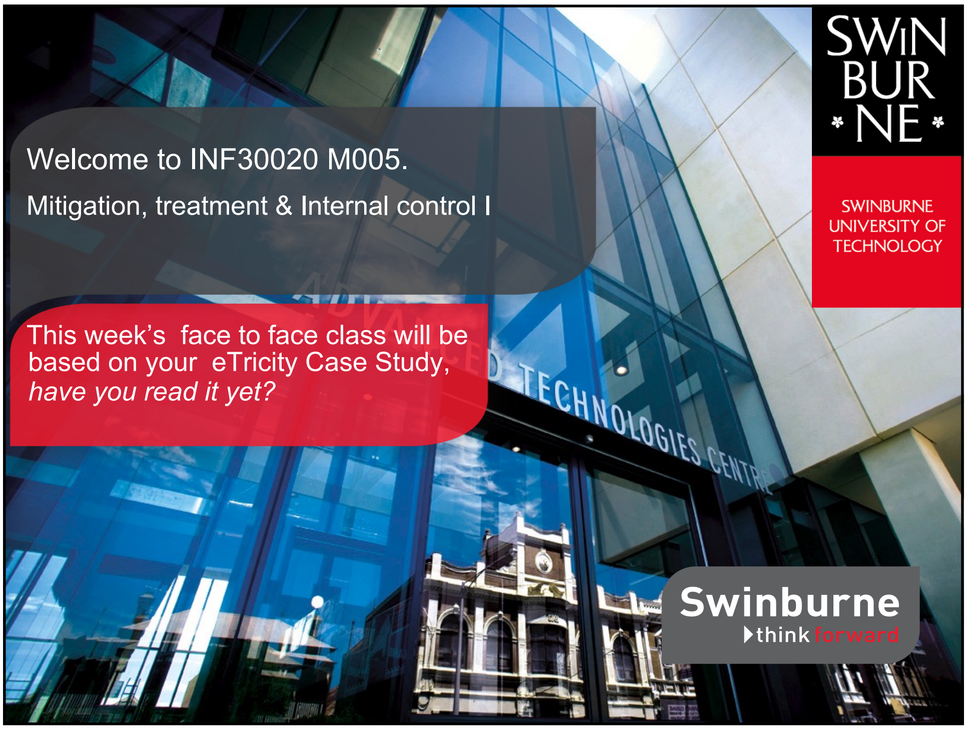


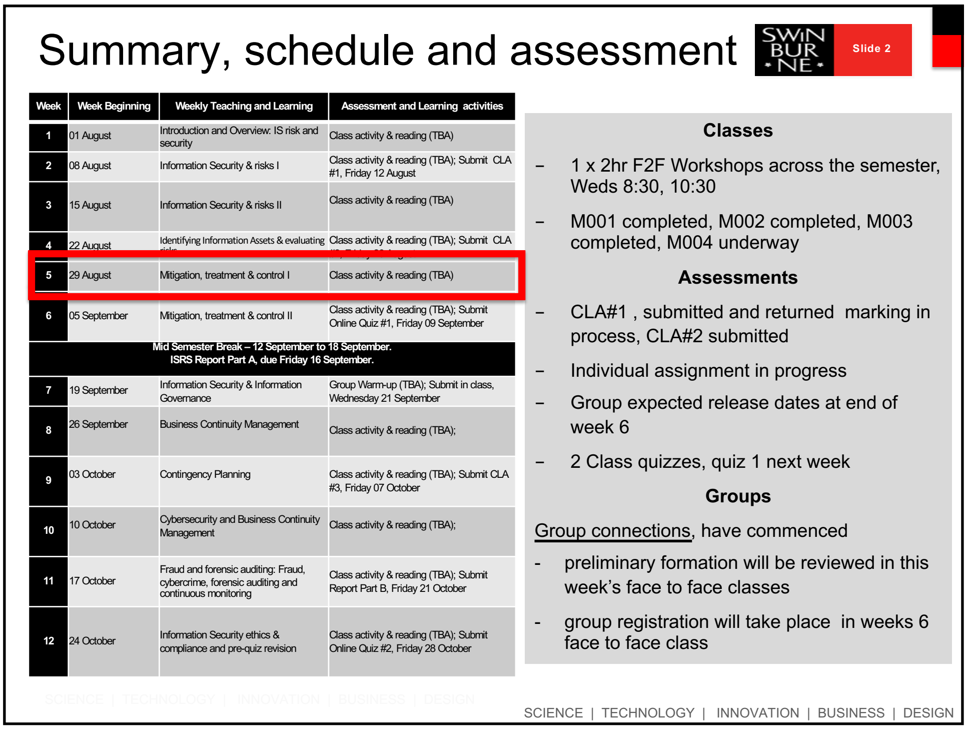
Welcome to INF30020 M005.

Mitigation, treatment & Internal control I

This week's face to face class will be based on your eTricity Case Study, *have you read it yet?*

SWINBURNE UNIVERSITY OF TECHNOLOGY

1



Summary, schedule and assessment

Slide 2

Week	Week Beginning	Weekly Teaching and Learning	Assessment and Learning activities
1	01 August	Introduction and Overview: IS risk and security	Class activity & reading (TBA)
2	08 August	Information Security & risks I	Class activity & reading (TBA); Submit CLA #1, Friday 12 August
3	15 August	Information Security & risks II	Class activity & reading (TBA)
4	22 August	Identifying Information Assets & evaluating risks	Class activity & reading (TBA); Submit CLA
5	29 August	Mitigation, treatment & control I	Class activity & reading (TBA)
6	05 September	Mitigation, treatment & control II	Class activity & reading (TBA); Submit Online Quiz #1, Friday 09 September
Mid Semester Break – 12 September to 18 September. ISRS Report Part A, due Friday 16 September.			
7	19 September	Information Security & Information Governance	Group Warm-up (TBA); Submit in class, Wednesday 21 September
8	26 September	Business Continuity Management	Class activity & reading (TBA);
9	03 October	Contingency Planning	Class activity & reading (TBA); Submit CLA #3, Friday 07 October
10	10 October	Cybersecurity and Business Continuity Management	Class activity & reading (TBA);
11	17 October	Fraud and forensic auditing: Fraud, cybercrime, forensic auditing and continuous monitoring	Class activity & reading (TBA); Submit Report Part B, Friday 21 October
12	24 October	Information Security ethics & compliance and pre-quiz revision	Class activity & reading (TBA); Submit Online Quiz #2, Friday 28 October

Classes

- 1 x 2hr F2F Workshops across the semester, Weds 8:30, 10:30
- M001 completed, M002 completed, M003 completed, M004 underway

Assessments

- CLA#1 , submitted and returned marking in process, CLA#2 submitted
- Individual assignment in progress
- Group expected release dates at end of week 6
- 2 Class quizzes, quiz 1 next week

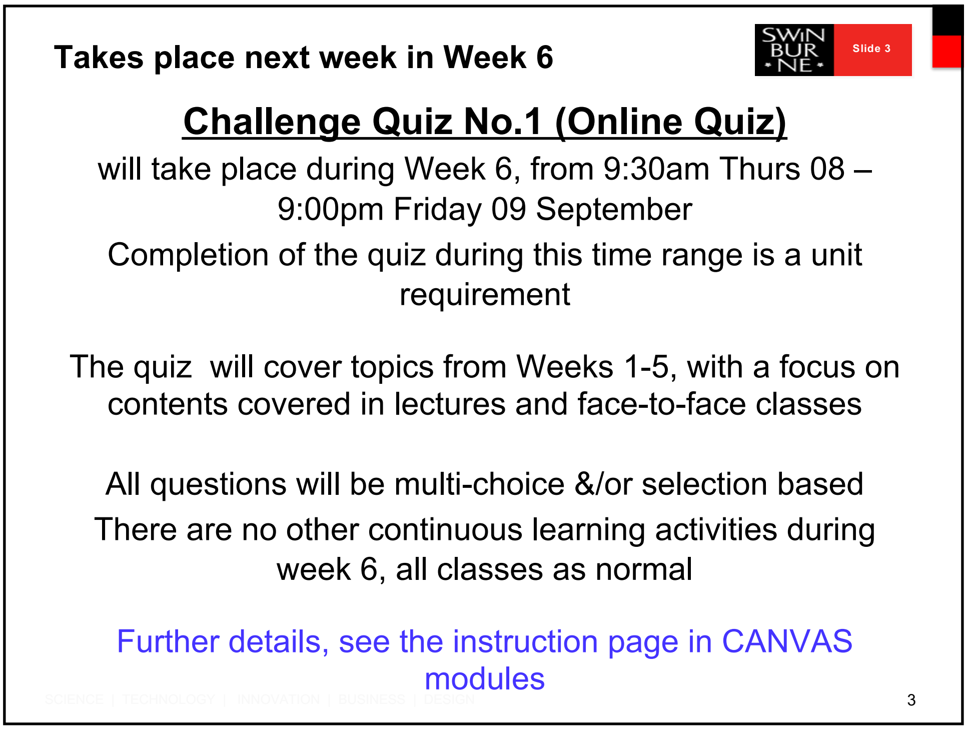
Groups

Group connections, have commenced

- preliminary formation will be reviewed in this week's face to face classes
- group registration will take place in weeks 6 face to face class

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

2



Takes place next week in Week 6

SWiN BUR NE Slide 3

Challenge Quiz No.1 (Online Quiz)

will take place during Week 6, from 9:30am Thurs 08 – 9:00pm Friday 09 September

Completion of the quiz during this time range is a unit requirement

The quiz will cover topics from Weeks 1-5, with a focus on contents covered in lectures and face-to-face classes

All questions will be multi-choice &/or selection based

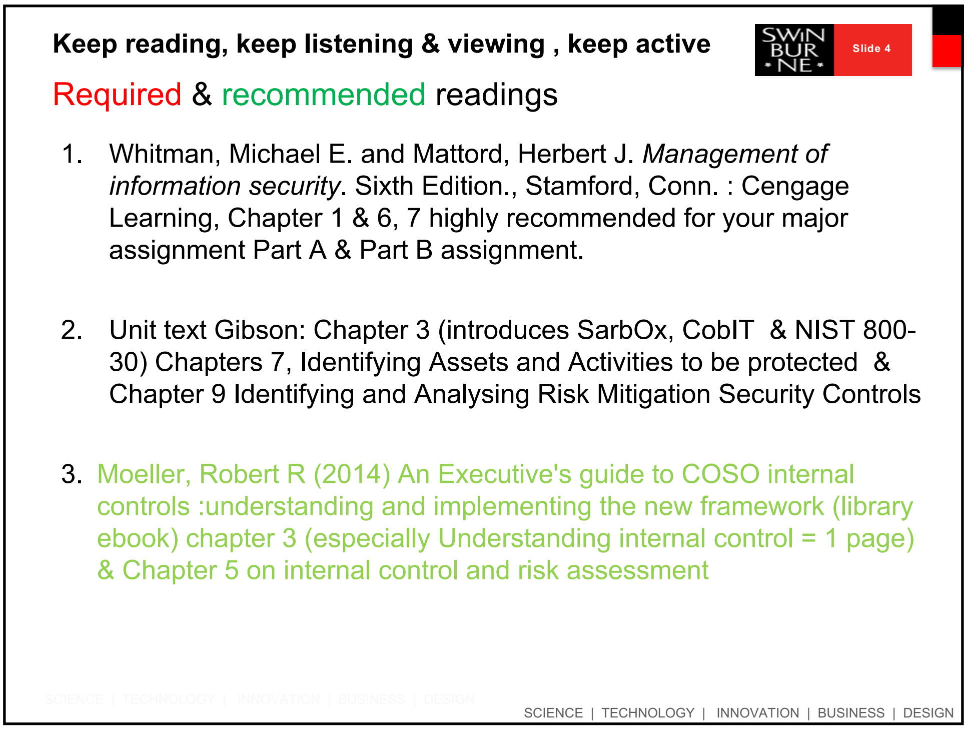
There are no other continuous learning activities during week 6, all classes as normal

Further details, see the instruction page in CANVAS modules

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

3

3



Keep reading, keep listening & viewing , keep active

SWiN BUR NE Slide 4

Required & recommended readings

1. Whitman, Michael E. and Mattord, Herbert J. *Management of information security*. Sixth Edition., Stamford, Conn. : Cengage Learning, Chapter 1 & 6, 7 highly recommended for your major assignment Part A & Part B assignment.

2. Unit text Gibson: Chapter 3 (introduces SarbOx, CobIT & NIST 800-30) Chapters 7, Identifying Assets and Activities to be protected & Chapter 9 Identifying and Analysing Risk Mitigation Security Controls

3. Moeller, Robert R (2014) An Executive's guide to COSO internal controls :understanding and implementing the new framework (library ebook) chapter 3 (especially Understanding internal control = 1 page) & Chapter 5 on internal control and risk assessment

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

4

Recommended readings

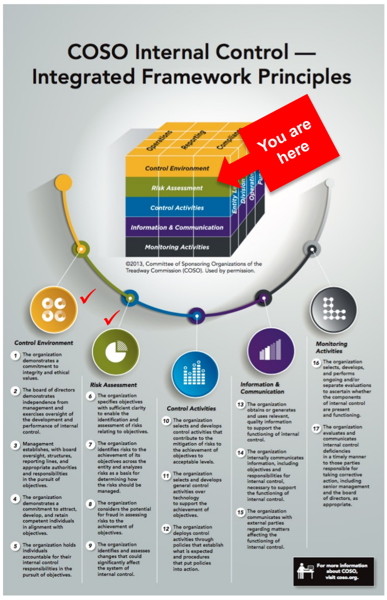
Work with COSO,

Helping to build out your assignment research base

No need to purchase – just use those resources that are freely available

https://www.coso.org/SitePages/Home.aspx

Executive Summary (2017)
Risk Appetite–Critical to Success (2020)
ERM Risk Assessment in Practice (2012)
Update to the Internal Control Framework (2013)



©2013, Committee of Sponsoring Organizations of the Treadway Commission (COSO). Used by permission.

Control Environment

1 The organization demonstrates a commitment to integrity and ethical values.

2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

4 The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

5 The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk Assessment

6 The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

7 The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

8 The organization considers the potential for fraud in assessing risks to the achievement of objectives.

9 The organization identifies and assesses changes that could significantly affect the system of internal control.

Control Activities

10 The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

11 The organization selects and develops general control activities over technology to support the achievement of objectives.

12 The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Information & Communication

13 The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

14 The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

15 The organization communicates with external parties regarding matters affecting the functioning of internal control.

Monitoring Activities

16 The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

17 The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

For more information about COSO, visit coso.org.

Keep reading, keep listening, keep active

SWIN BUR NE Slide 6

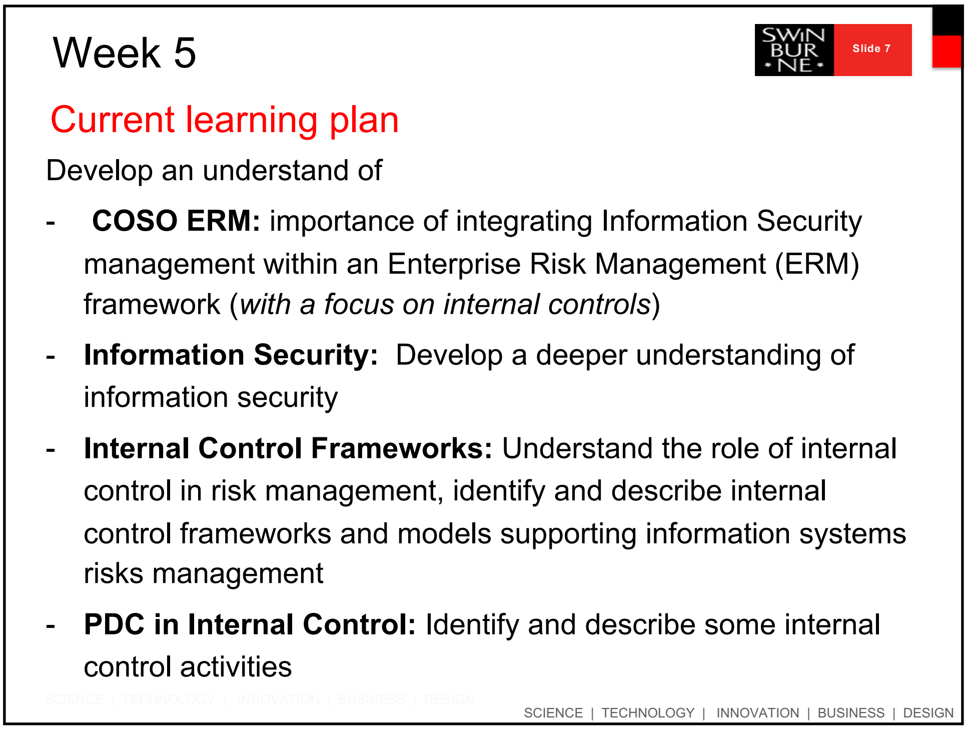
Required Standards

AS ISO 31000:2018 : Risk management – Guidelines *http://ezproxy.lib.swin.edu.au/login?url=https://subscriptions.techstreet.com/products/806031 (Links to an external site.)*

AS/NZS ISO/IEC 27005:2012 : Information technology - Security techniques - Information security risk management *http://ezproxy.lib.swin.edu.au/login?url=https://subscriptions.techstreet.com/products/862854 (Links to an external site.)*

NIST 800-30 r1, Guide for Conducting Risk Assessments https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Information Assets and Business Requirements (2011). The National Archives of the United Kingdom



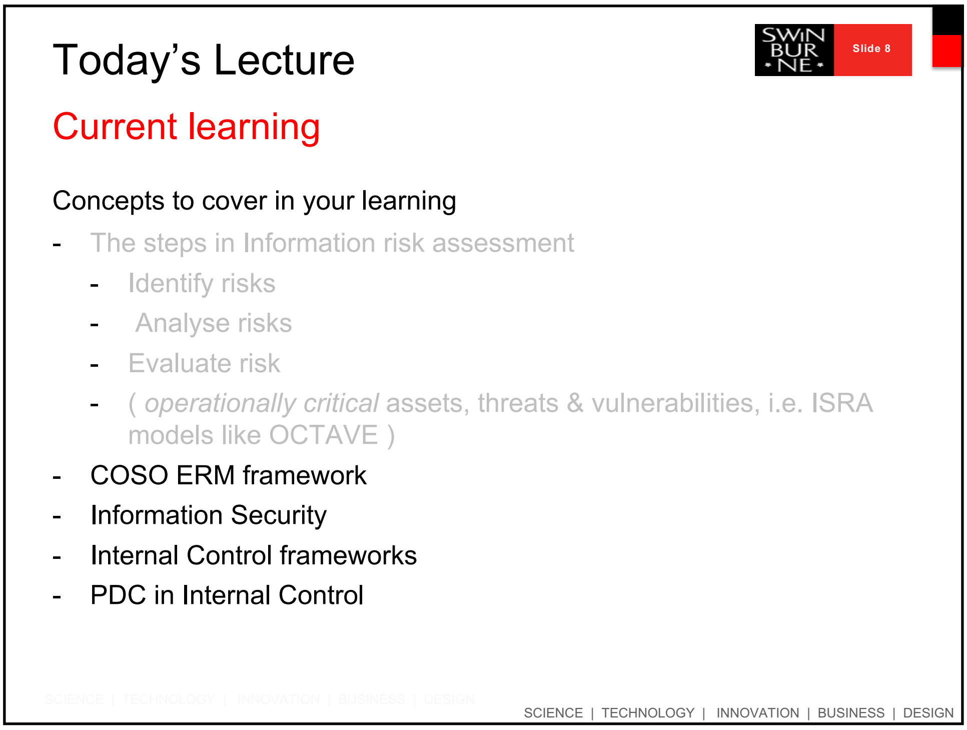
Week 5

Slide 7

Current learning plan

Develop an understand of

- **COSO ERM:** importance of integrating Information Security management within an Enterprise Risk Management (ERM) framework (*with a focus on internal controls*)
- **Information Security:** Develop a deeper understanding of information security
- **Internal Control Frameworks:** Understand the role of internal control in risk management, identify and describe internal control frameworks and models supporting information systems risks management
- **PDC in Internal Control:** Identify and describe some internal control activities



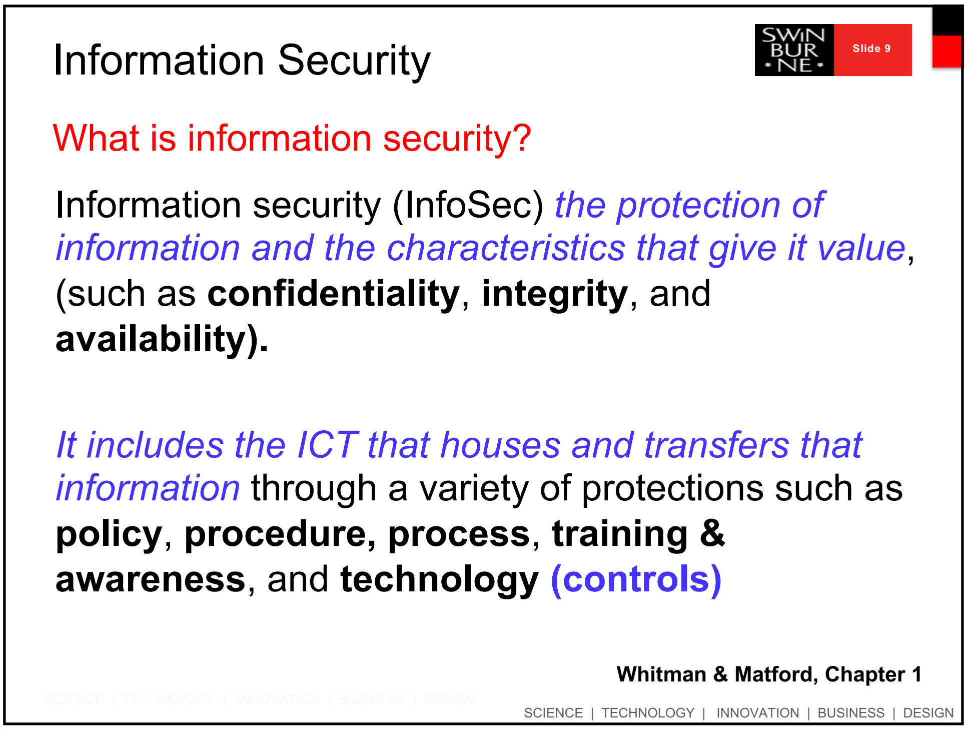
Today's Lecture

Slide 8

Current learning

Concepts to cover in your learning

- The steps in Information risk assessment
  - Identify risks
  - Analyse risks
  - Evaluate risk
  - (*operationally critical* assets, threats & vulnerabilities, i.e. ISRA models like OCTAVE)
- COSO ERM framework
- Information Security
- Internal Control frameworks
- PDC in Internal Control



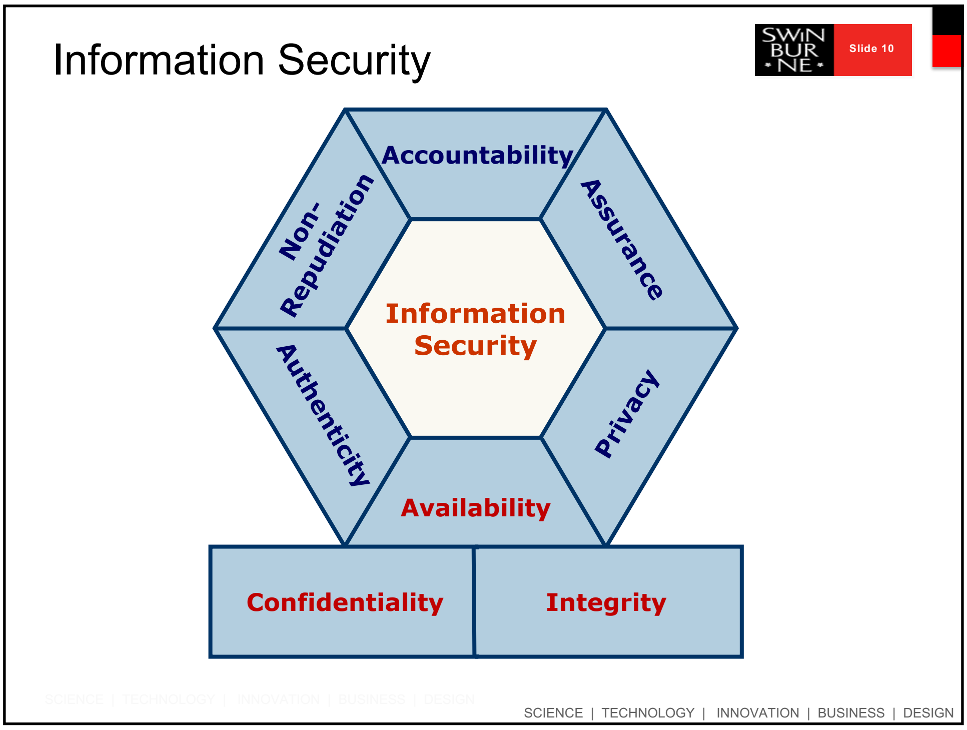
Information Security

What is information security?

Information security (InfoSec) *the protection of information and the characteristics that give it value*, (such as **confidentiality**, **integrity**, and **availability).**

It includes the ICT that houses and transfers that information through a variety of protections such as **policy**, **procedure, process**, **training & awareness**, and **technology (controls)**

Whitman & Matford, Chapter 1



Information Security

Information Security

Slide 11

- **Confidentiality** meaning that the information assets can be accessed and disclosed only by authorised parties (also refers to secrecy)
- **Integrity** meaning that the information assets can only be modified or deleted by authorised parties in authorised ways, therefore they are always complete and true
- **Availability** meaning that the information assets are accessible to the authorised parties in a timely manner
- **Non-repudiation (Legal Enforceability)** meaning the ability to “prove” that a sender sent or receiver received a message (or both), even if the sender or receiver wishes to deny it later
- **Authenticity** meaning both genuineness (not corrupted from the original) and validity (verifying the identity of a subject requesting the use) of an information asset.
- **Privacy** meaning to protect the confidentiality and identity of a user (compared to Confidentiality where the information asset itself is protected)
- **Accountability** meaning the ability to audit the level of protection provided for information assets and the ability to identify where the responsibility lies to provide such protection
- **Assurance** ***meaning the measurement of confidence in the level of protection of an information asset and the degree to which a particular control enforces information security policy requirements***

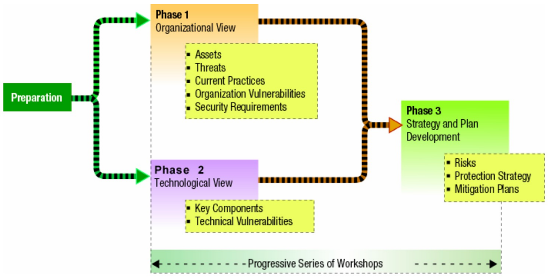
SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

11

Information Security

Slide 12

Information Systems Risk Assessment methodologies



An organization makes information protection decisions based on operational risks and security practices

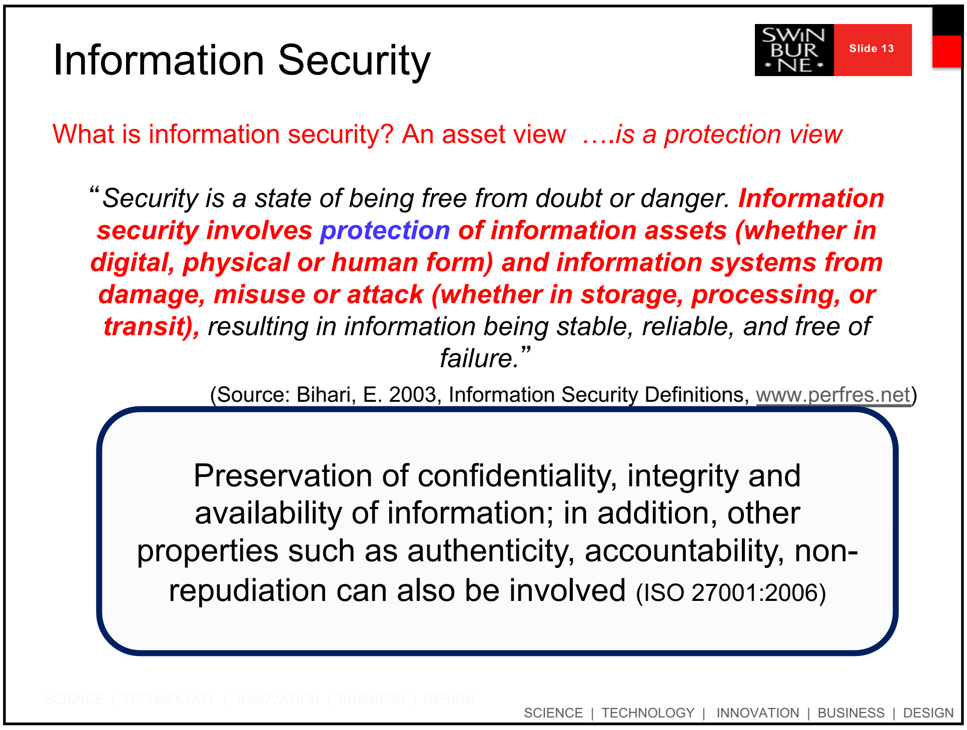
OCTAVE is a risk- based strategic assessment and planning technique for security.

US DoD and Carnegie Mellon

1. Identify assets and what is being done to protect those assets
2. Identify the critical assets and what is required to protect them
3. Identify vulnerabilities to critical assets
4. Identify threats to critical assets (and what is required to protect against them - *safeguarding*)

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

12



Information Security

Slide 13

What is information security? An asset view ….*is a protection view*

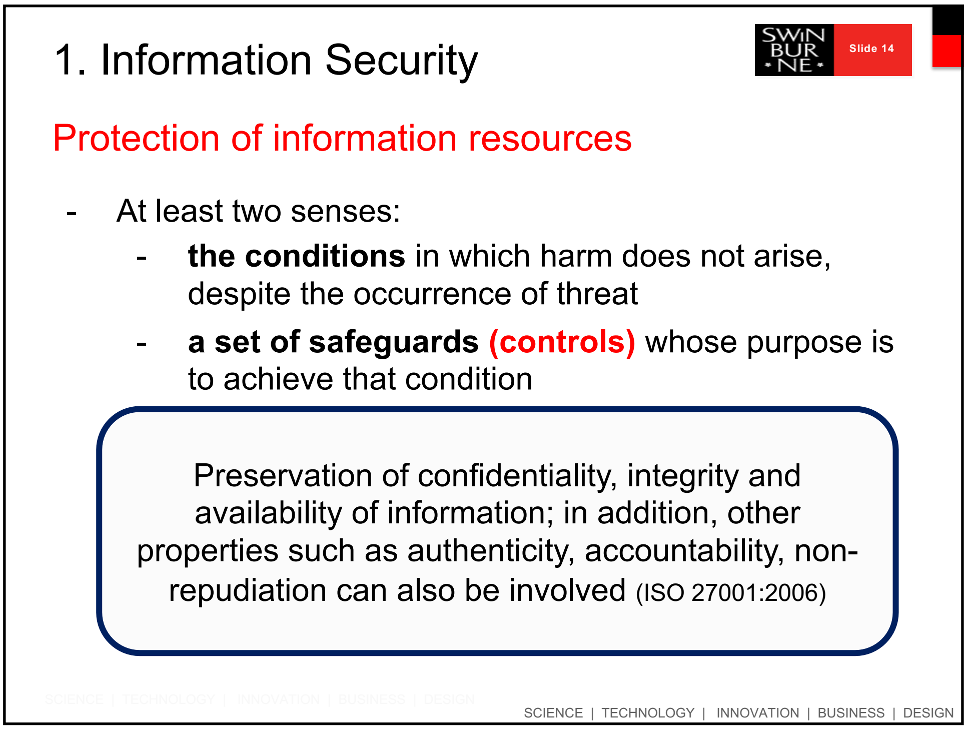
> *"Security is a state of being free from doubt or danger.* ***Information security involves protection of information assets (whether in digital, physical or human form) and information systems from damage, misuse or attack (whether in storage, processing, or transit),*** *resulting in information being stable, reliable, and free of failure."*

(Source: Bihari, E. 2003, Information Security Definitions, www.perfres.net)

Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation can also be involved (ISO 27001:2006)

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

13



1. Information Security

Slide 14

Protection of information resources

- At least two senses:
  - **the conditions** in which harm does not arise, despite the occurrence of threat
  - **a set of safeguards (controls)** whose purpose is to achieve that condition

Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation can also be involved (ISO 27001:2006)

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

14

Information Security

Assurance and control

***Assurance** meaning the measurement of confidence in the level of protection of an information asset **(i.e. conditions preventing harm)** and the degree to which a particular **control** **(i.e. a set of safeguards)** enforces **information security** requirements*

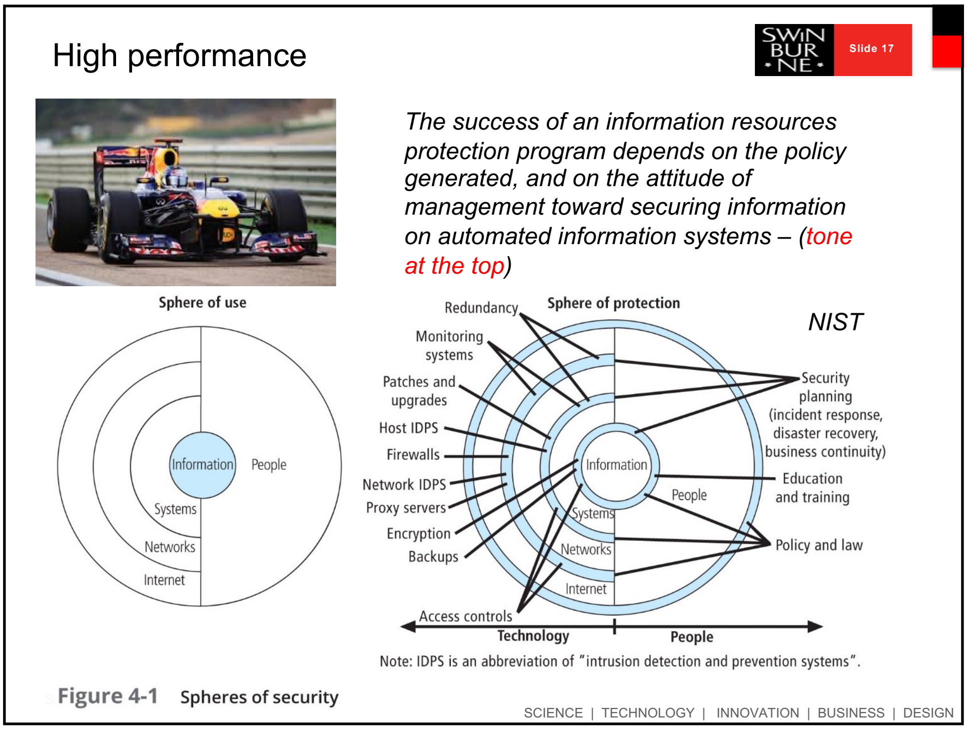
SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

High performance

"You don't put brakes on a car to go slower, you put brakes on a car to go faster, more safely

…along the same lines, IT security is not meant to slow down a company, but rather to enhance and facilitate... safer growth. "

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN



High performance

Slide 17

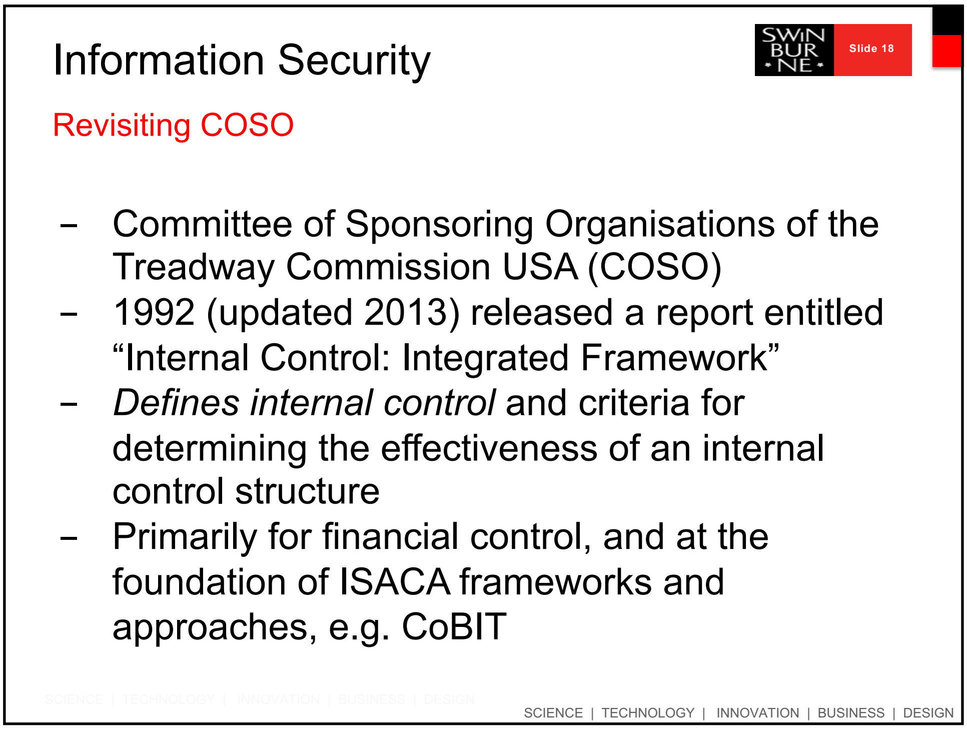
The success of an information resources protection program depends on the policy generated, and on the attitude of management toward securing information on automated information systems – (tone at the top)

Note: IDPS is an abbreviation of "intrusion detection and prevention systems".

Figure 4-1 Spheres of security

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

17



Information Security

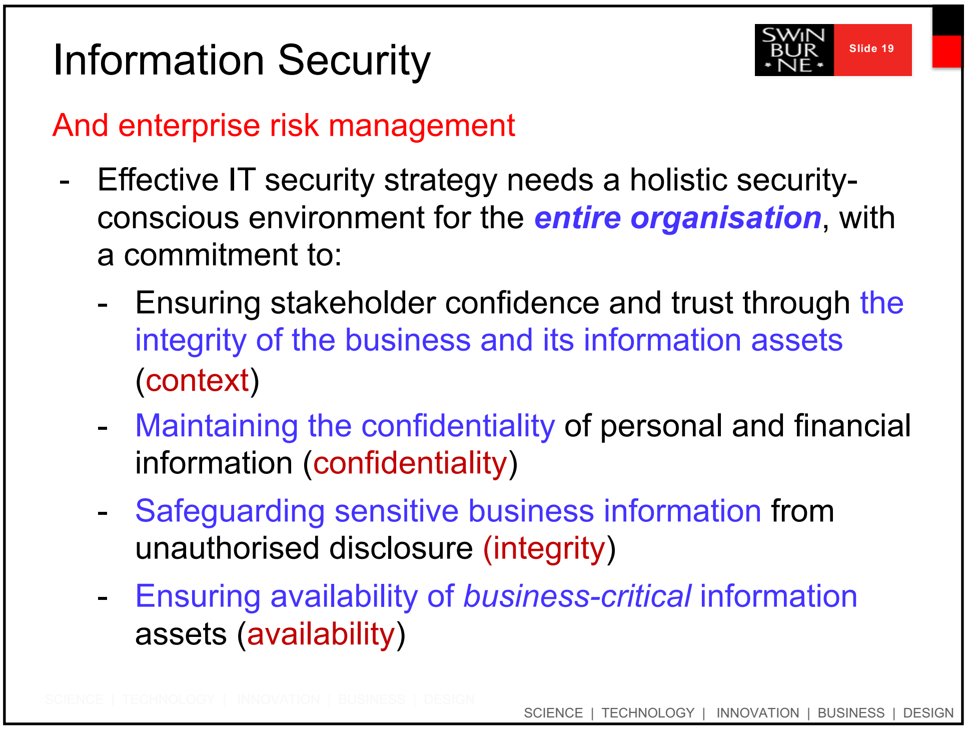
Slide 18

Revisiting COSO

- Committee of Sponsoring Organisations of the Treadway Commission USA (COSO)
- 1992 (updated 2013) released a report entitled "Internal Control: Integrated Framework"
- *Defines internal control* and criteria for determining the effectiveness of an internal control structure
- Primarily for financial control, and at the foundation of ISACA frameworks and approaches, e.g. CoBIT

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

18

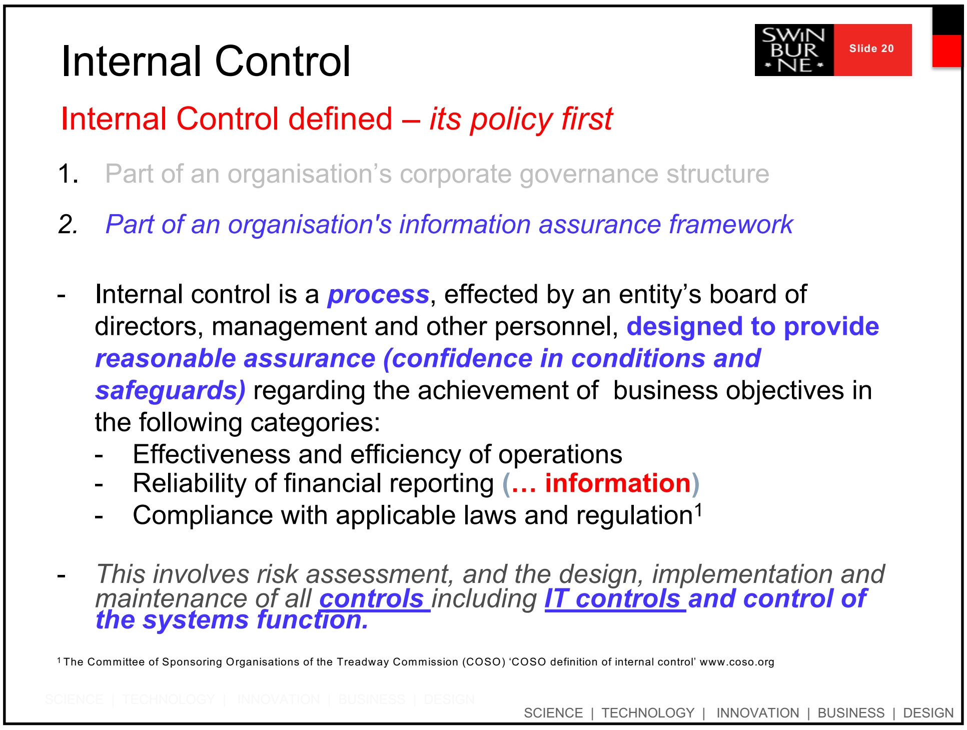


Information Security

Slide 19

And enterprise risk management

- Effective IT security strategy needs a holistic security-conscious environment for the ***entire organisation***, with a commitment to:
  - Ensuring stakeholder confidence and trust through the integrity of the business and its information assets (context)
  - Maintaining the confidentiality of personal and financial information (confidentiality)
  - Safeguarding sensitive business information from unauthorised disclosure (integrity)
  - Ensuring availability of *business-critical* information assets (availability)



Internal Control

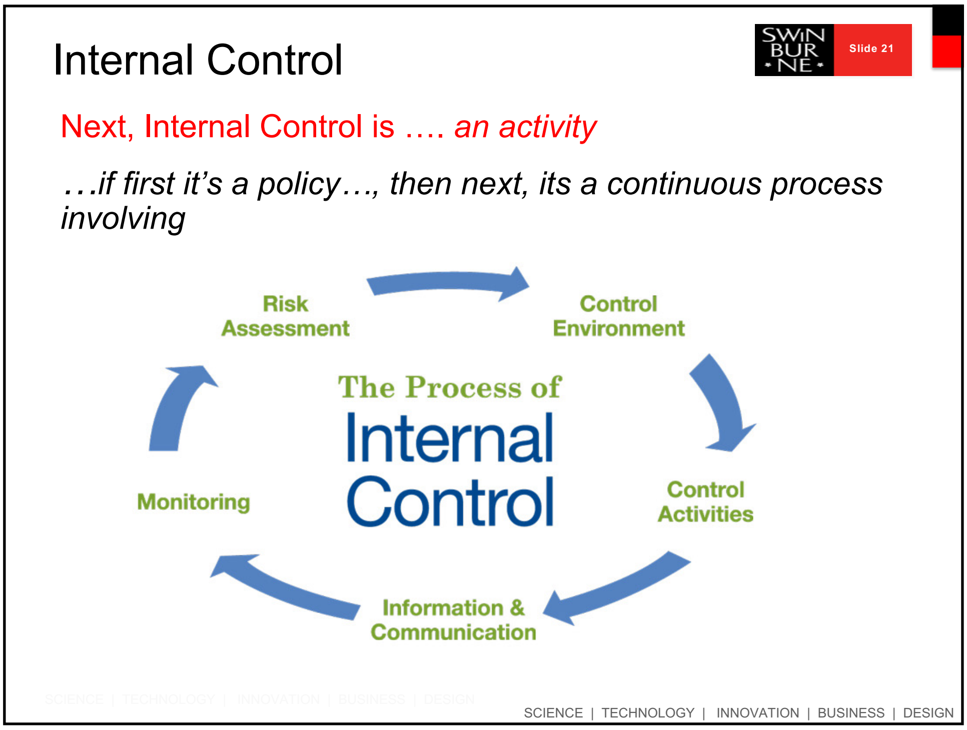
Slide 20

Internal Control defined – *its policy first*

1. Part of an organisation's corporate governance structure
2. *Part of an organisation's information assurance framework*

- Internal control is a ***process***, effected by an entity's board of directors, management and other personnel, **designed to provide *reasonable assurance (confidence in conditions and safeguards)*** regarding the achievement of business objectives in the following categories:
  - Effectiveness and efficiency of operations
  - Reliability of financial reporting (**… information**)
  - Compliance with applicable laws and regulation[1]
- *This involves risk assessment, and the design, implementation and maintenance of all* ***controls*** *including* ***IT controls and control of the systems function.***

[1] The Committee of Sponsoring Organisations of the Treadway Commission (COSO) 'COSO definition of internal control' www.coso.org



Internal Control

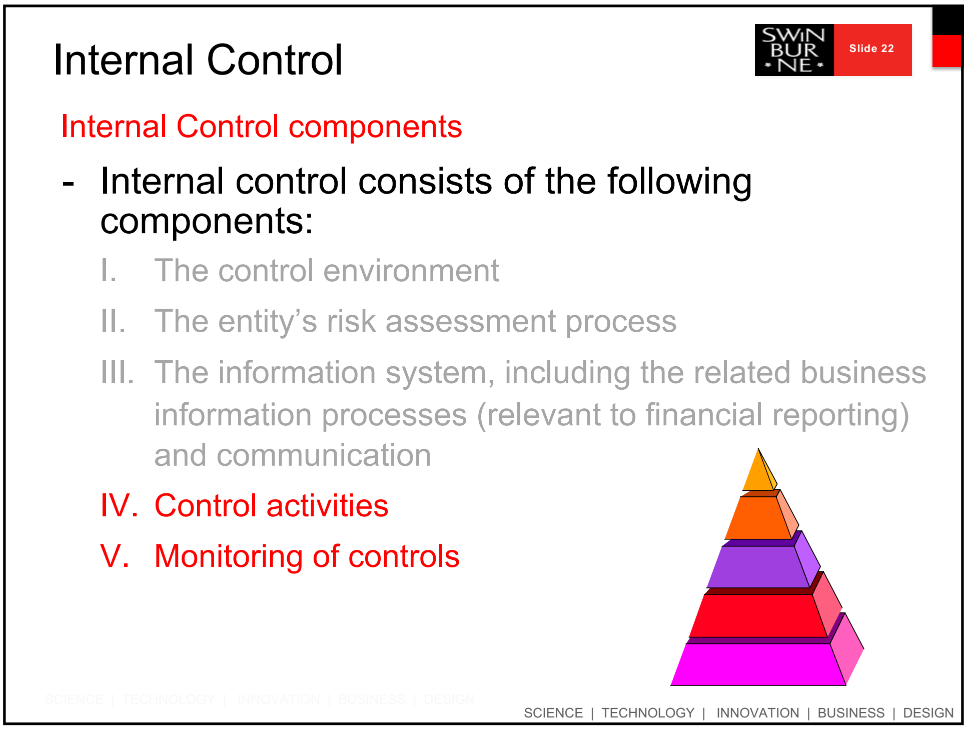
SWIN BUR NE Slide 21

Next, Internal Control is …. *an activity*

…if first it's a policy…, then next, its a continuous process involving

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

21



Internal Control

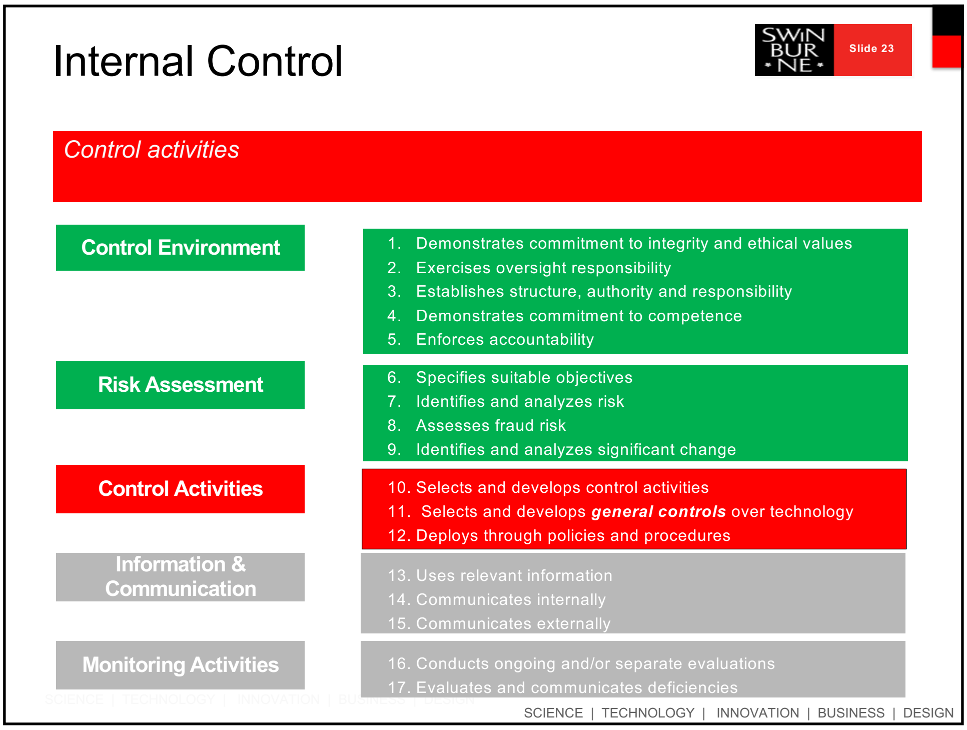
SWIN BUR NE Slide 22

Internal Control components

- Internal control consists of the following components:
  - I. The control environment
  - II. The entity's risk assessment process
  - III. The information system, including the related business information processes (relevant to financial reporting) and communication
  - IV. Control activities
  - V. Monitoring of controls

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

22



Internal Control

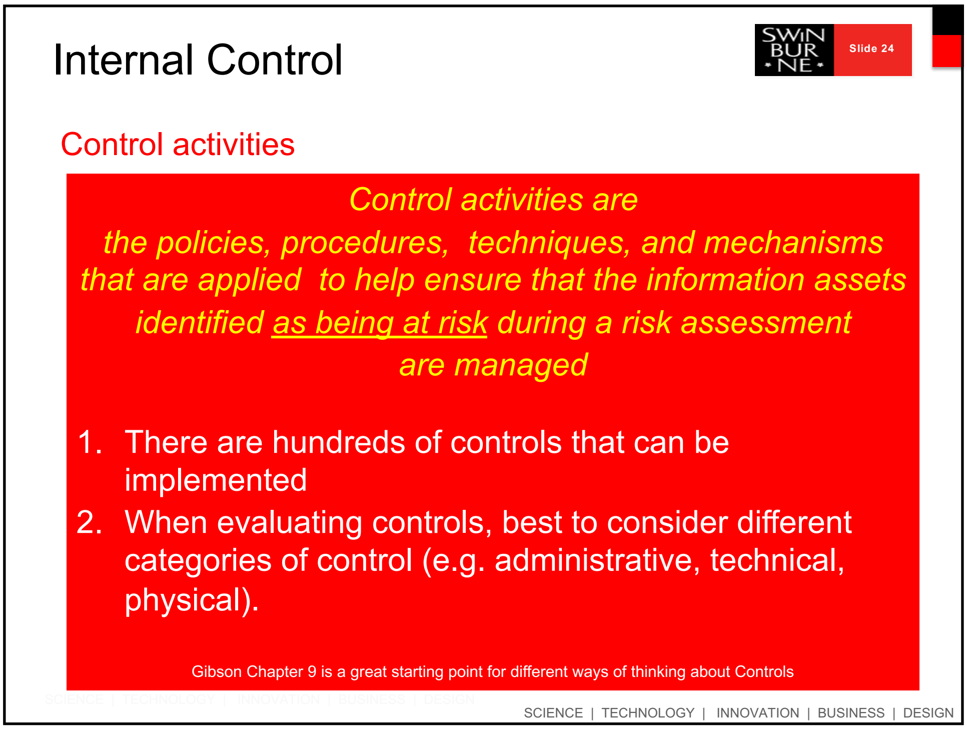
SWIN BUR NE Slide 23

Control activities

Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops ***general controls*** over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

23



Internal Control

SWIN BUR NE Slide 24

Control activities

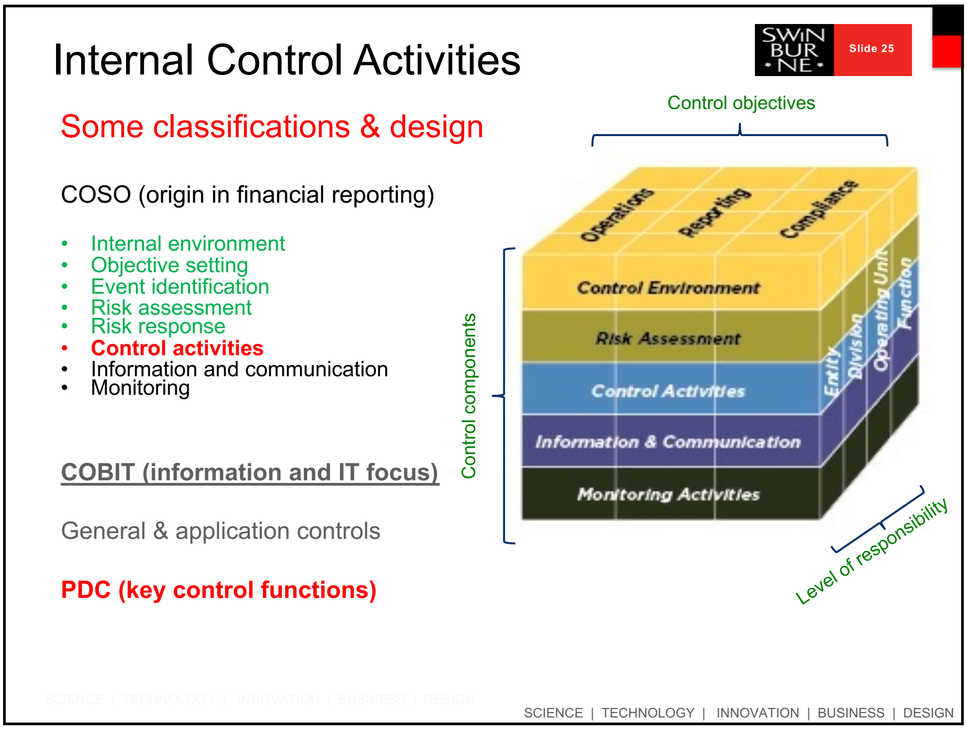
Control activities are the policies, procedures, techniques, and mechanisms that are applied to help ensure that the information assets identified as being at risk during a risk assessment are managed

1. There are hundreds of controls that can be implemented
2. When evaluating controls, best to consider different categories of control (e.g. administrative, technical, physical).

Gibson Chapter 9 is a great starting point for different ways of thinking about Controls

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

24



Internal Control Activities

Slide 25

Some classifications & design

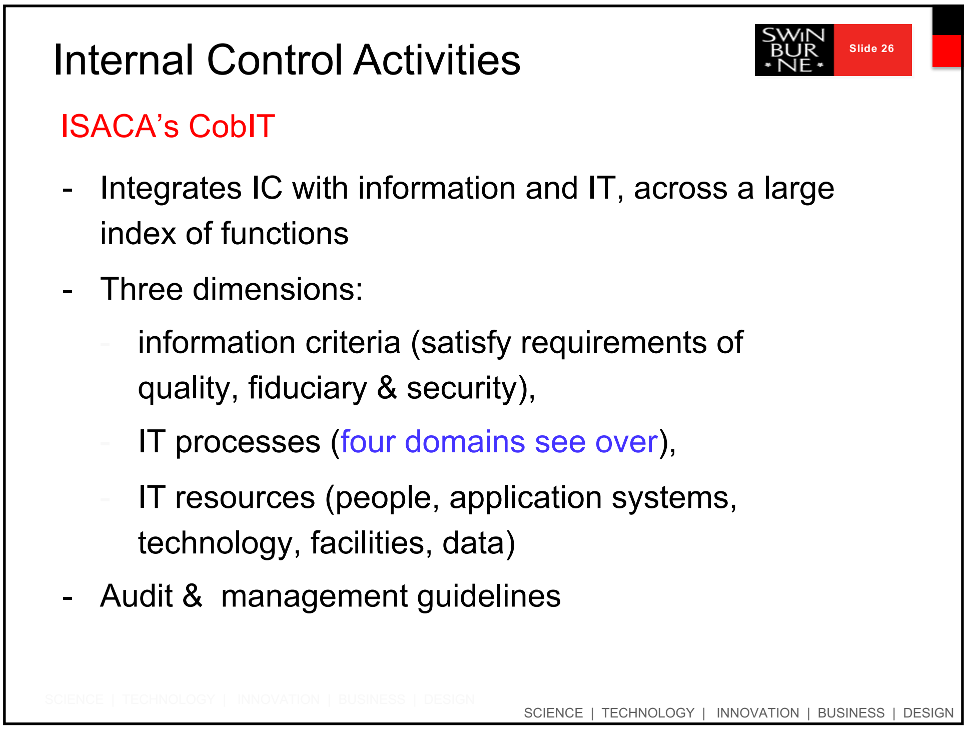
COSO (origin in financial reporting)

- Internal environment
- Objective setting
- Event identification
- Risk assessment
- Risk response
- **Control activities**
- Information and communication
- Monitoring

COBIT (information and IT focus)

General & application controls

PDC (key control functions)

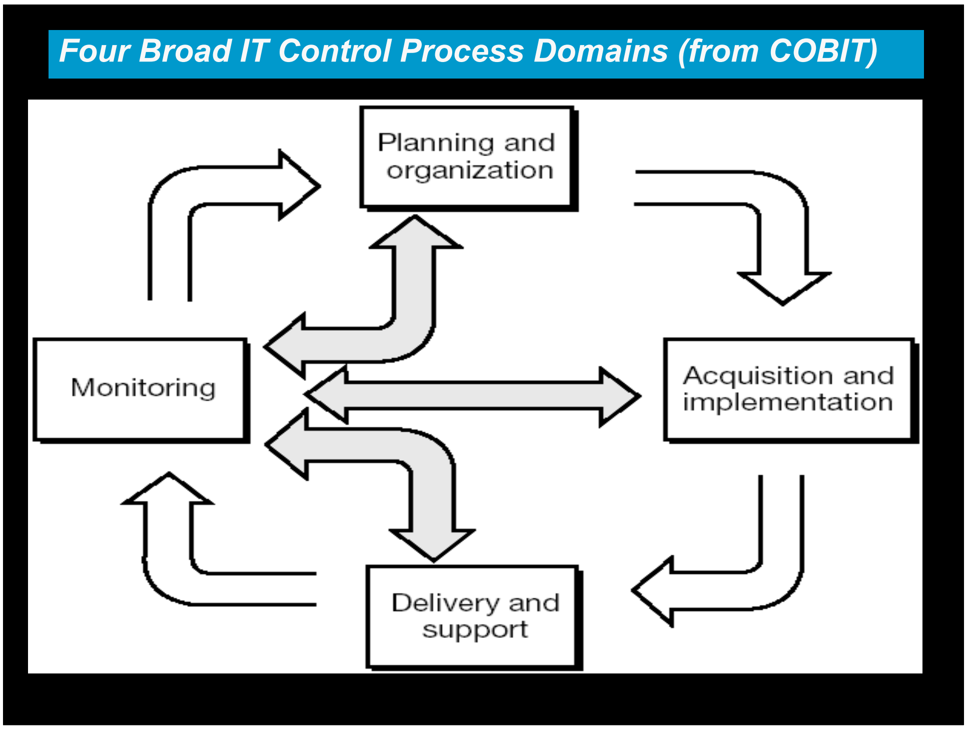


Internal Control Activities

Slide 26

ISACA’s CobIT

- Integrates IC with information and IT, across a large index of functions
- Three dimensions:
  - information criteria (satisfy requirements of quality, fiduciary & security),
  - IT processes (four domains see over),
  - IT resources (people, application systems, technology, facilities, data)
- Audit & management guidelines



Four Broad IT Control Process Domains (from COBIT)

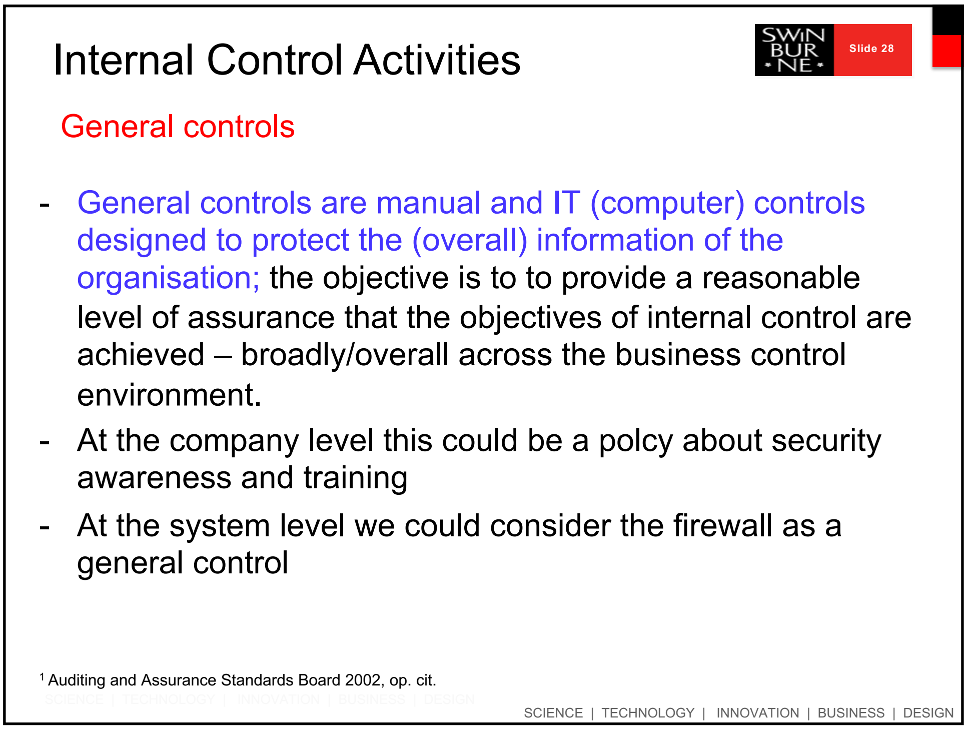
Planning and organization

Acquisition and implementation

Delivery and support

Monitoring

27



Internal Control Activities

SWiN BUR NE Slide 28

General controls

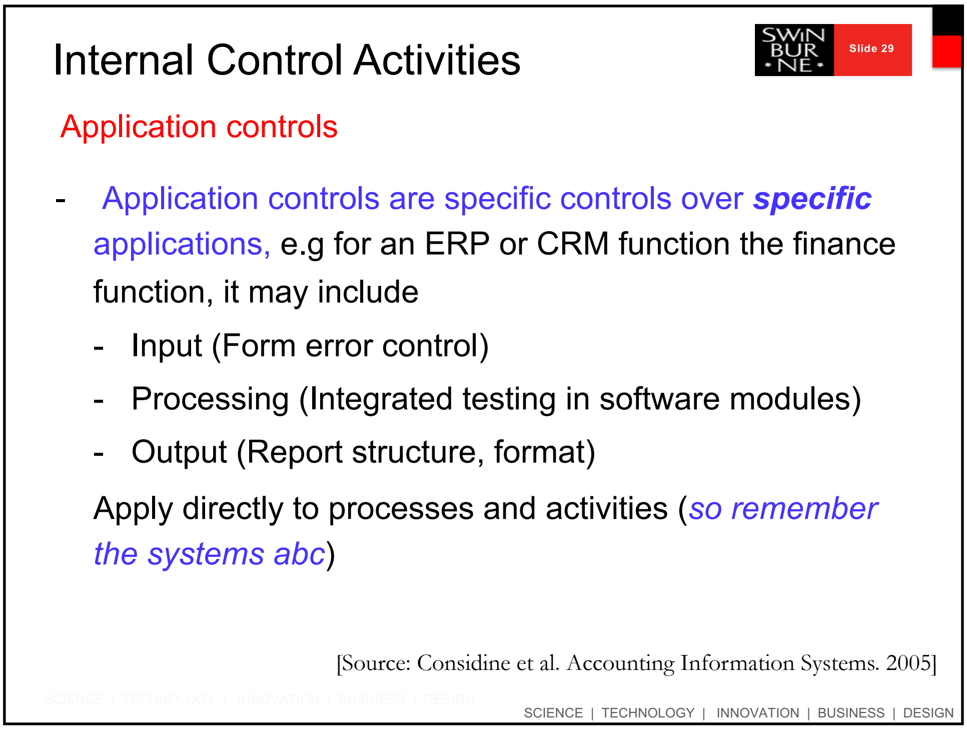
- General controls are manual and IT (computer) controls designed to protect the (overall) information of the organisation; the objective is to to provide a reasonable level of assurance that the objectives of internal control are achieved – broadly/overall across the business control environment.
- At the company level this could be a polcy about security awareness and training
- At the system level we could consider the firewall as a general control

[1] Auditing and Assurance Standards Board 2002, op. cit.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

28



Internal Control Activities

Slide 29

Application controls

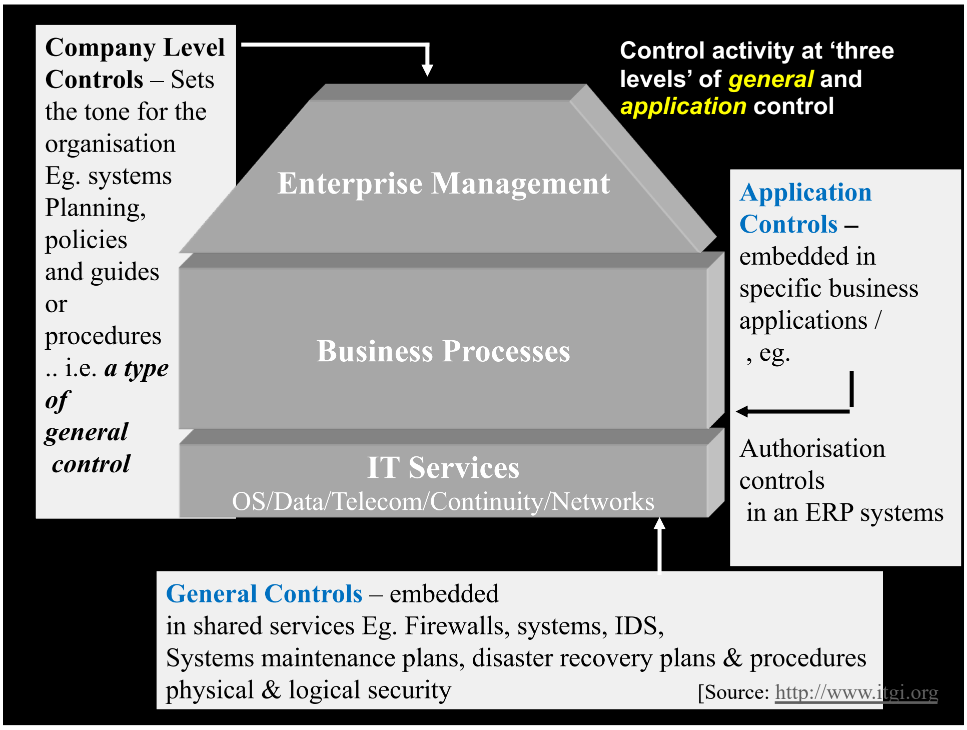
- Application controls are specific controls over ***specific*** applications, e.g for an ERP or CRM function the finance function, it may include
  - Input (Form error control)
  - Processing (Integrated testing in software modules)
  - Output (Report structure, format)

  Apply directly to processes and activities (*so remember the systems abc*)

[Source: Considine et al. Accounting Information Systems. 2005]

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

29



Company Level Controls – Sets the tone for the organisation Eg. systems Planning, policies and guides or procedures .. i.e. ***a type of general control***

Control activity at 'three levels' of *general* and *application* control

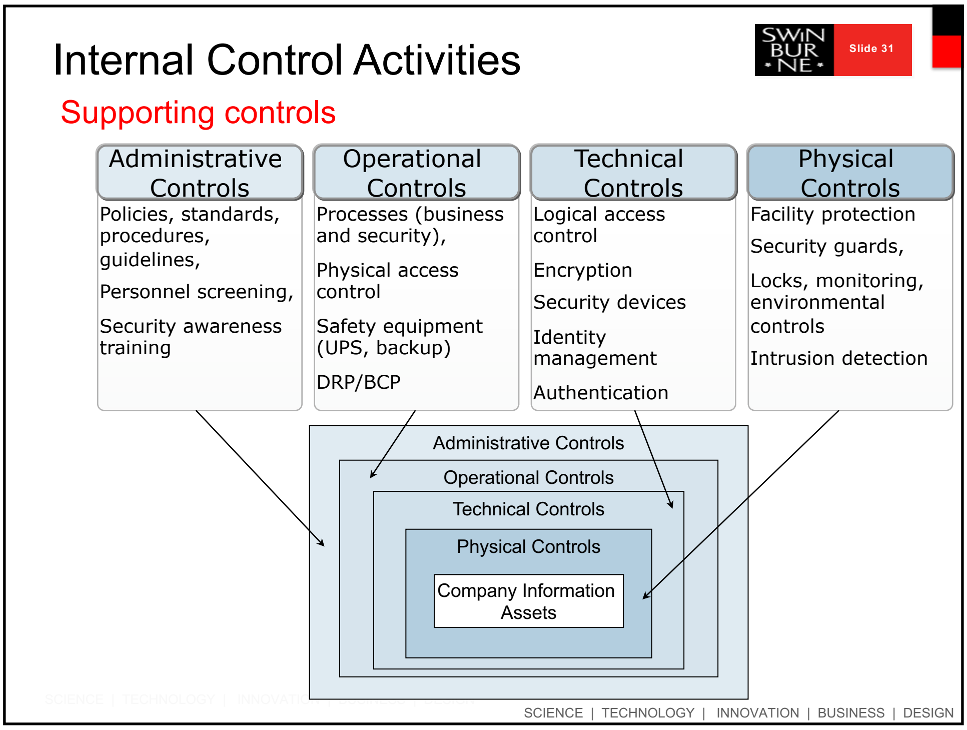
Application Controls – embedded in specific business applications / , eg.

Authorisation controls in an ERP systems

General Controls – embedded in shared services Eg. Firewalls, systems, IDS, Systems maintenance plans, disaster recovery plans & procedures physical & logical security

[Source: http://www.itgi.org

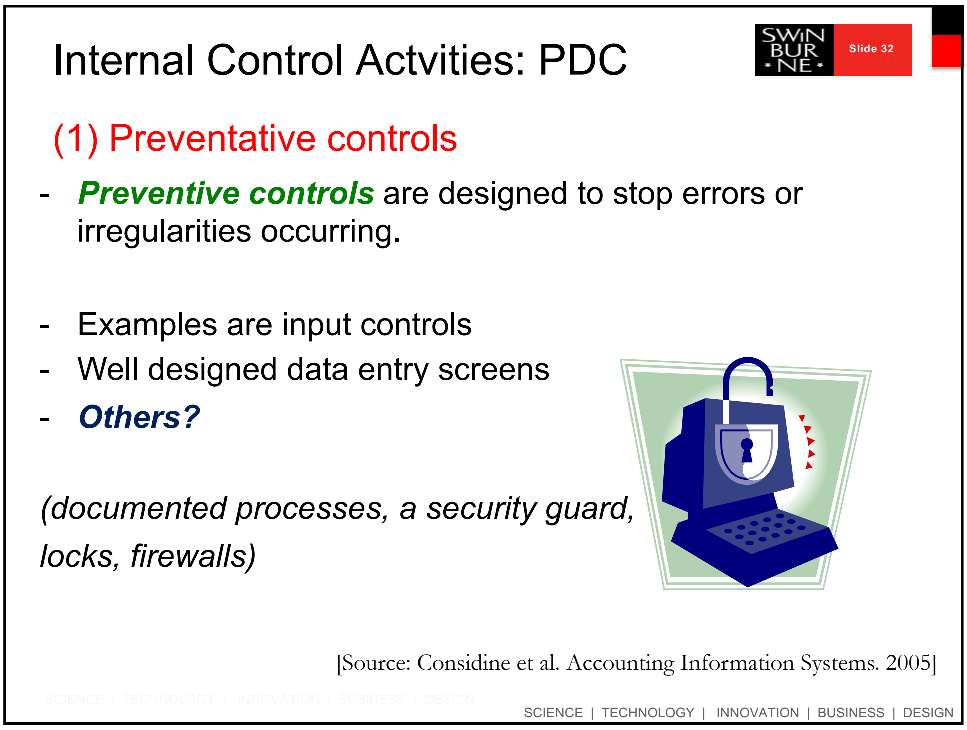
30



Internal Control Activities

Supporting controls

Administrative Controls	Operational Controls	Technical Controls	Physical Controls
Policies, standards, procedures, guidelines, Personnel screening, Security awareness training	Processes (business and security), Physical access control Safety equipment (UPS, backup) DRP/BCP	Logical access control Encryption Security devices Identity management Authentication	Facility protection Security guards, Locks, monitoring, environmental controls Intrusion detection



Internal Control Actvities: PDC

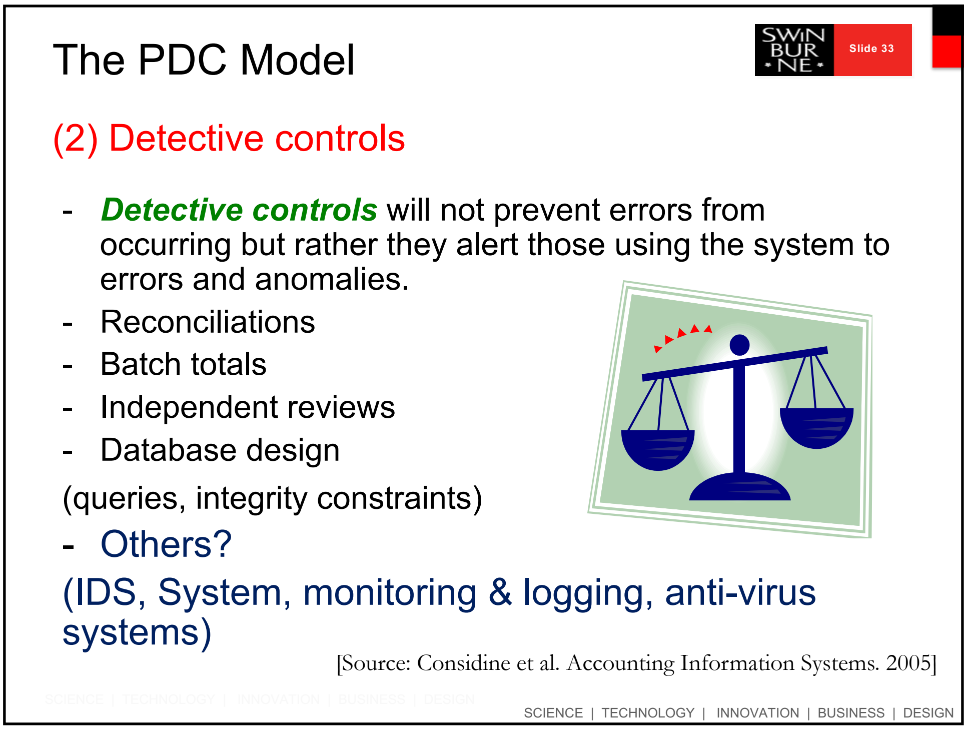
(1) Preventative controls

- ***Preventive controls*** are designed to stop errors or irregularities occurring.

- Examples are input controls
- Well designed data entry screens
- ***Others?***

(documented processes, a security guard, locks, firewalls)

[Source: Considine et al. Accounting Information Systems. 2005]



The PDC Model

Slide 33

(2) Detective controls

- ***Detective controls*** will not prevent errors from occurring but rather they alert those using the system to errors and anomalies.
- Reconciliations
- Batch totals
- Independent reviews
- Database design

(queries, integrity constraints)

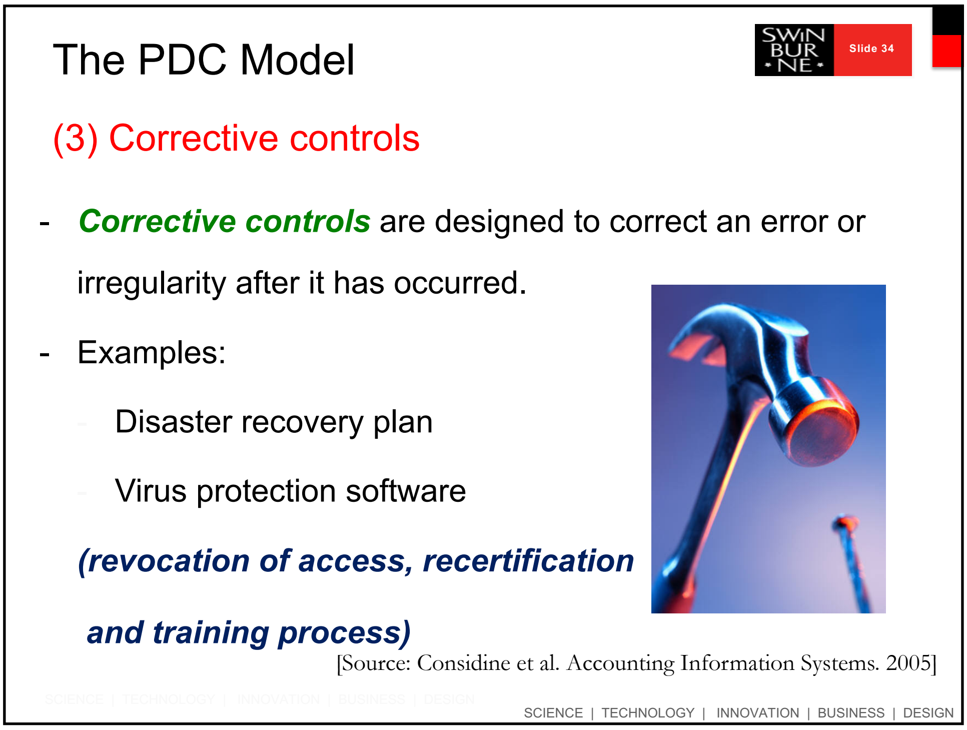
- Others?

(IDS, System, monitoring & logging, anti-virus systems)

[Source: Considine et al. Accounting Information Systems. 2005]

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

33



The PDC Model

Slide 34

(3) Corrective controls

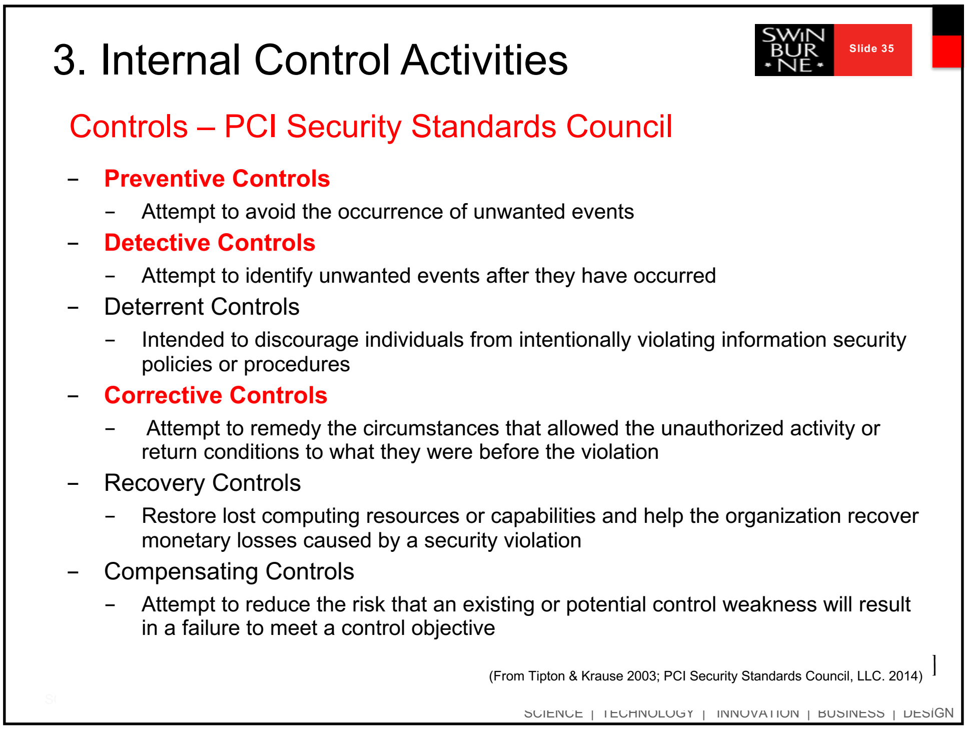
- ***Corrective controls*** are designed to correct an error or irregularity after it has occurred.
- Examples:
  - Disaster recovery plan
  - Virus protection software

(revocation of access, recertification and training process)

[Source: Considine et al. Accounting Information Systems. 2005]

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

34



Slide 35

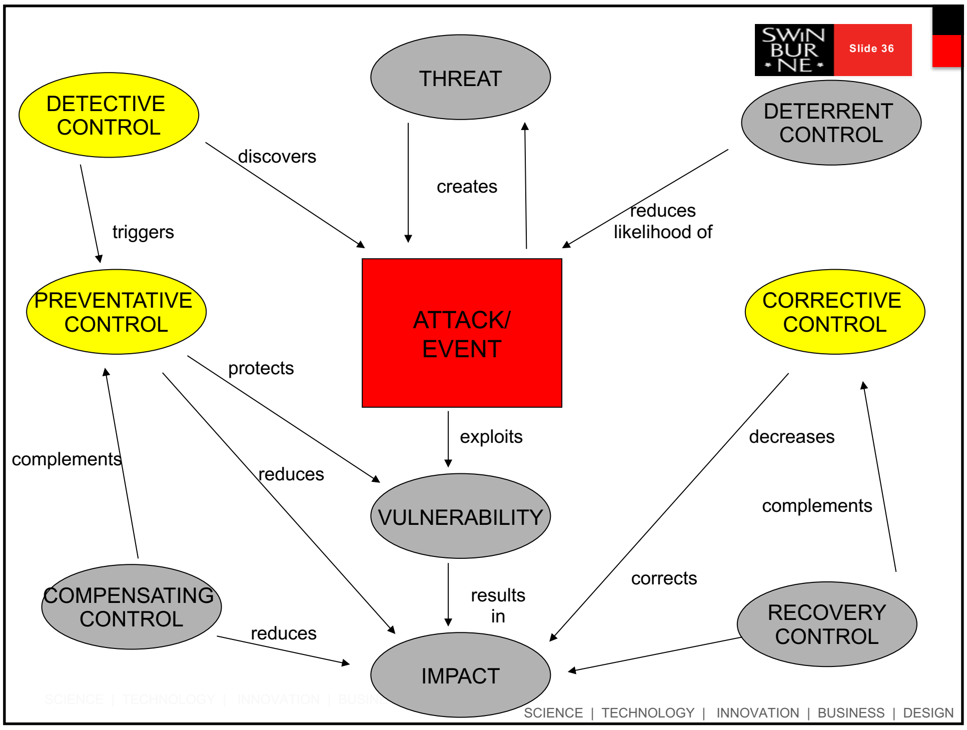
3. Internal Control Activities

Controls – PCI Security Standards Council

- **Preventive Controls**
  - Attempt to avoid the occurrence of unwanted events
- **Detective Controls**
  - Attempt to identify unwanted events after they have occurred
- Deterrent Controls
  - Intended to discourage individuals from intentionally violating information security policies or procedures
- **Corrective Controls**
  - Attempt to remedy the circumstances that allowed the unauthorized activity or return conditions to what they were before the violation
- Recovery Controls
  - Restore lost computing resources or capabilities and help the organization recover monetary losses caused by a security violation
- Compensating Controls
  - Attempt to reduce the risk that an existing or potential control weakness will result in a failure to meet a control objective

(From Tipton & Krause 2003; PCI Security Standards Council, LLC. 2014)

35



Slide 36

DETECTIVE CONTROL

THREAT

DETERRENT CONTROL

discovers

creates

reduces likelihood of

triggers

PREVENTATIVE CONTROL

ATTACK/ EVENT

CORRECTIVE CONTROL

protects

exploits

decreases

complements

reduces

VULNERABILITY

complements

corrects

COMPENSATING CONTROL

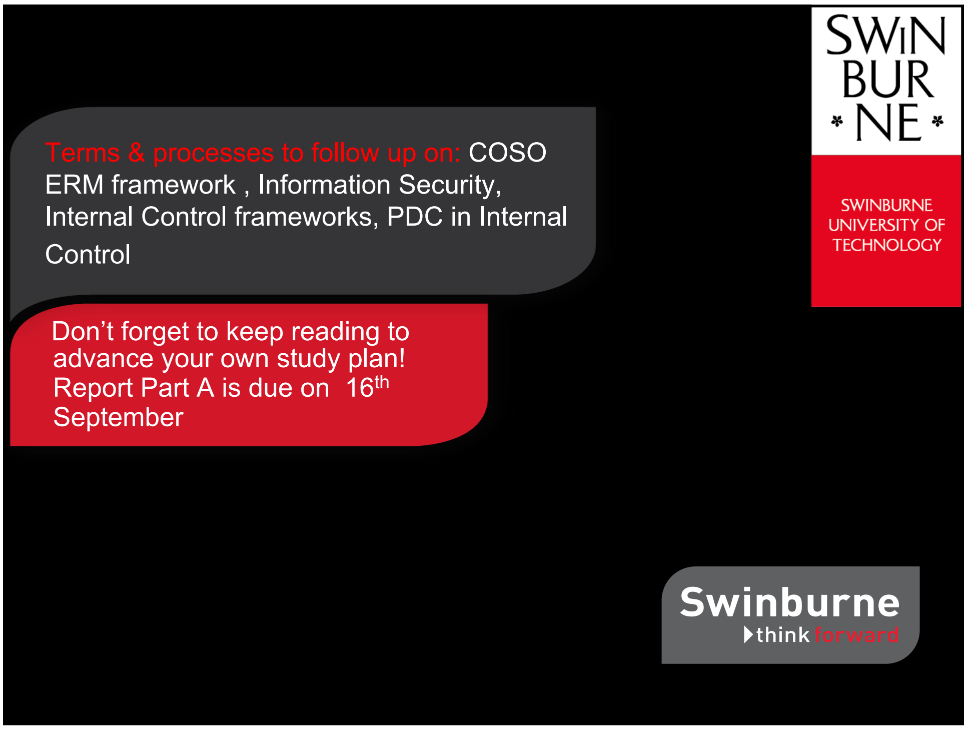
results in

RECOVERY CONTROL

reduces

IMPACT

36



Terms & processes to follow up on: COSO ERM framework , Information Security, Internal Control frameworks, PDC in Internal Control

Don’t forget to keep reading to advance your own study plan! Report Part A is due on 16th September