Welcome to INF30020 Lecture 6

Recorded lecture: Mitigation, treatment & Internal control

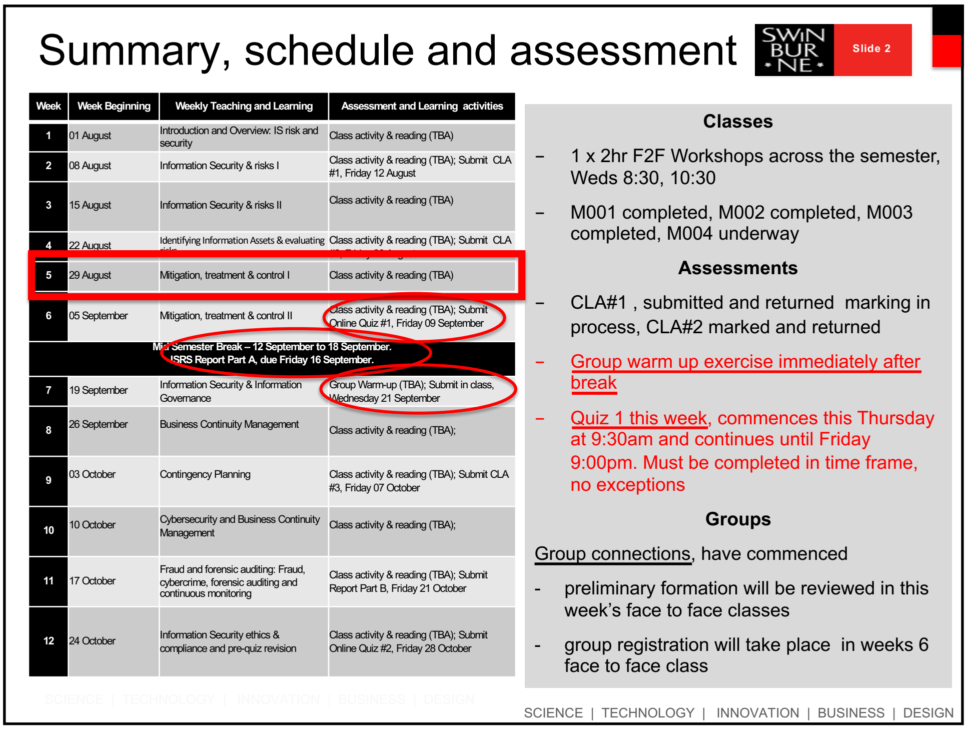
(1) Internal control, (2) risk treatment plans, (3) IS audit & assurance

SWINBURNE UNIVERSITY OF TECHNOLOGY

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

CRICOS Provider: 00111D | TOID: 3059

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 #2, Friday 26 August
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 marked and returned
- Group warm up exercise immediately after break
- Quiz 1 this week, commences this Thursday at 9:30am and continues until Friday 9:00pm. Must be completed in time frame, no exceptions

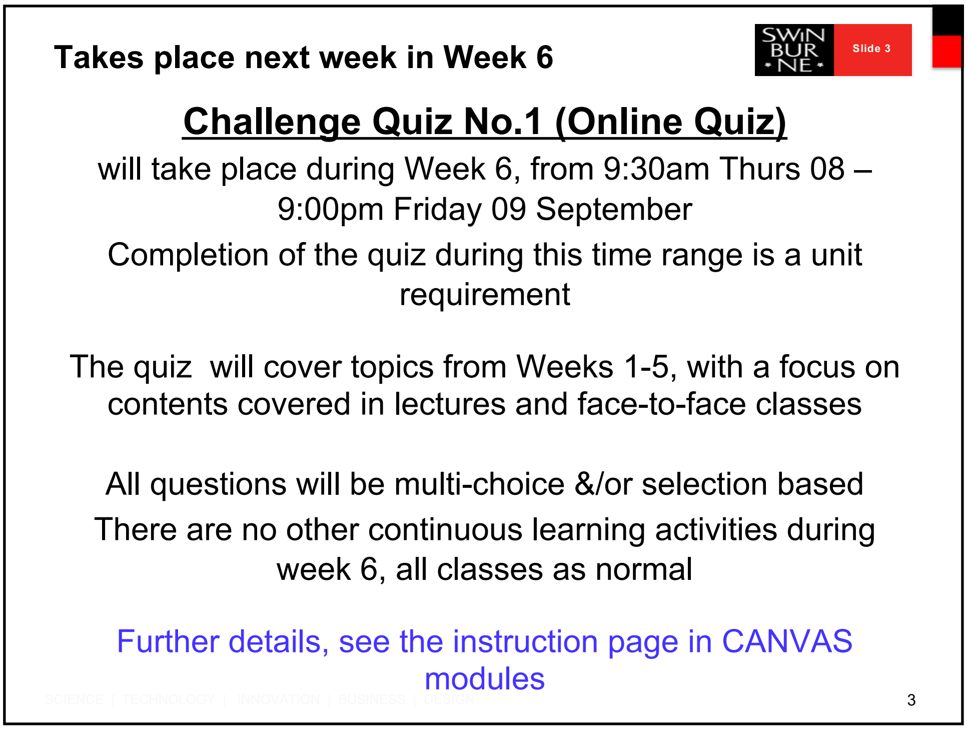
Groups

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

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

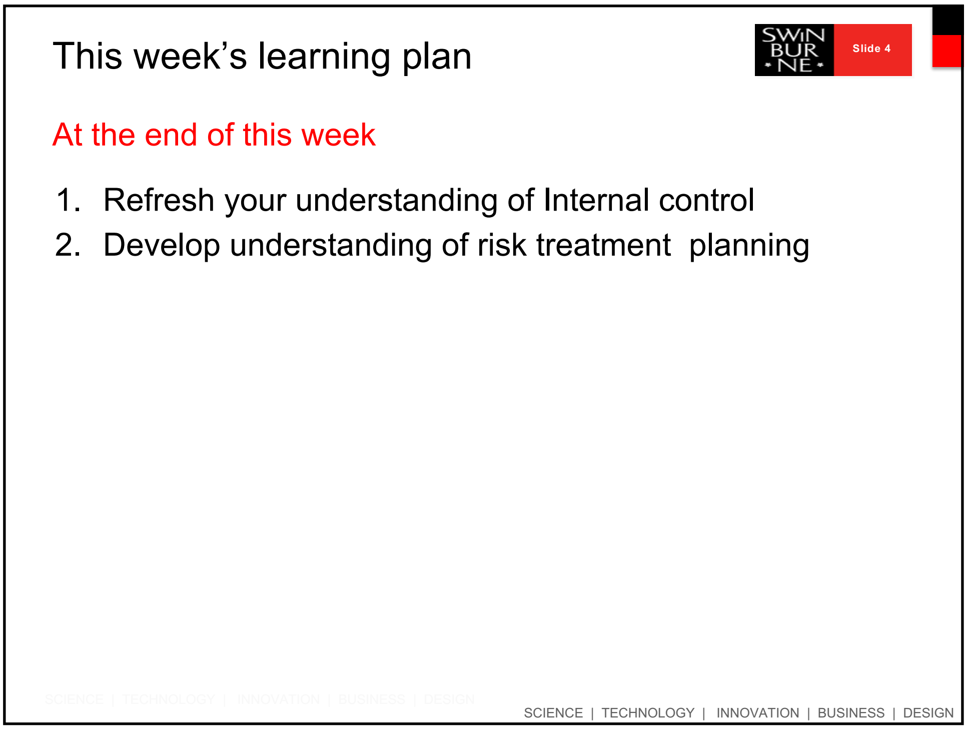
There are no other continuous learning activities during week 6, all classes as normal

Further details, see the instruction page in CANVAS modules

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

3

3



This week's learning plan

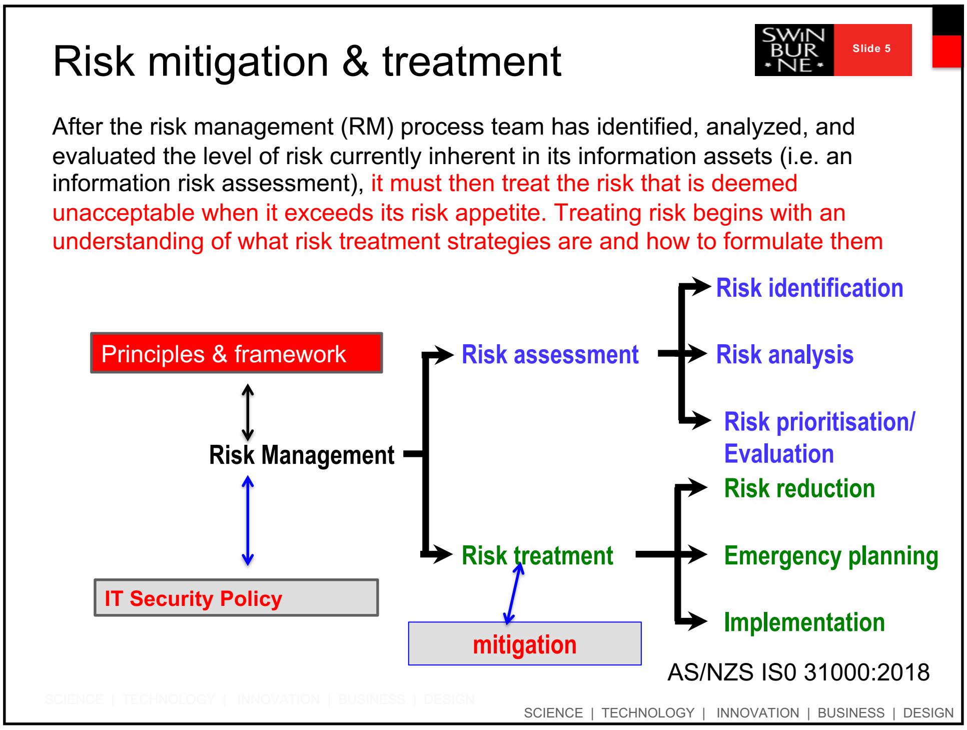
Slide 4

At the end of this week

1. Refresh your understanding of Internal control
2. Develop understanding of risk treatment planning

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

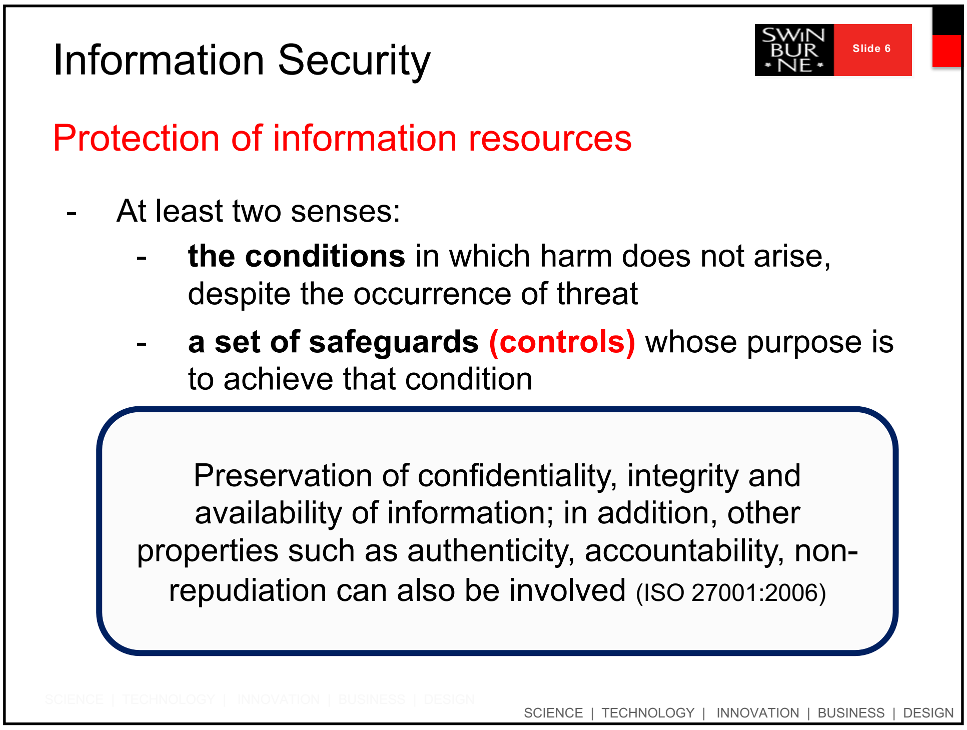
4



Risk mitigation & treatment

After the risk management (RM) process team has identified, analyzed, and evaluated the level of risk currently inherent in its information assets (i.e. an information risk assessment), it must then treat the risk that is deemed unacceptable when it exceeds its risk appetite. Treating risk begins with an understanding of what risk treatment strategies are and how to formulate them

AS/NZS IS0 31000:2018

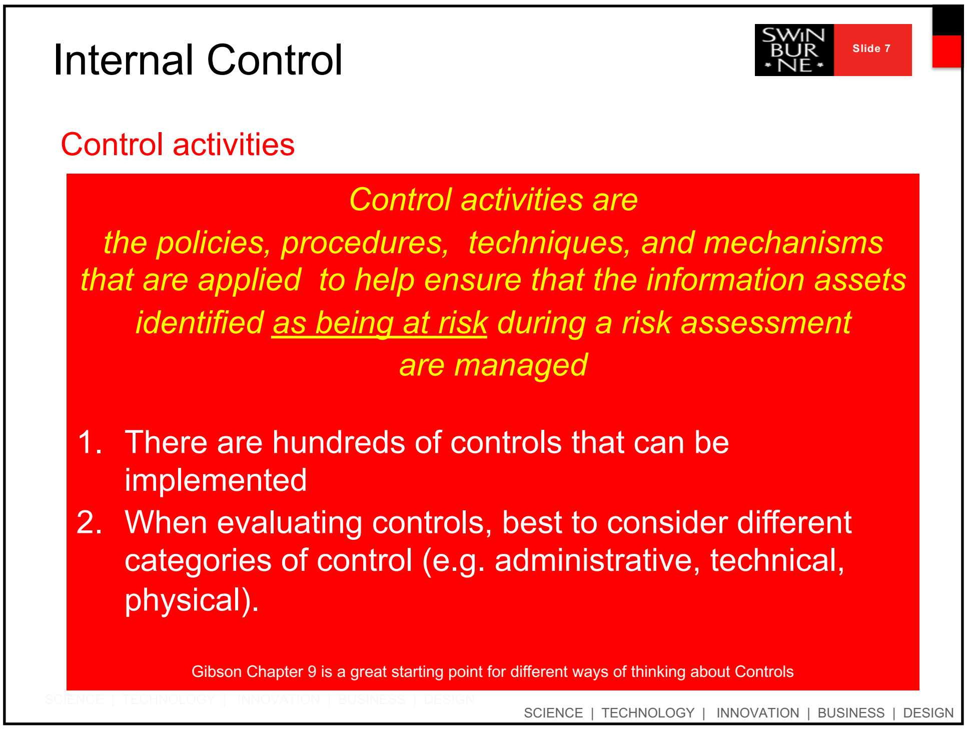


Information Security

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)



Internal Control

SWIN BUR NE
Slide 7

Control activities

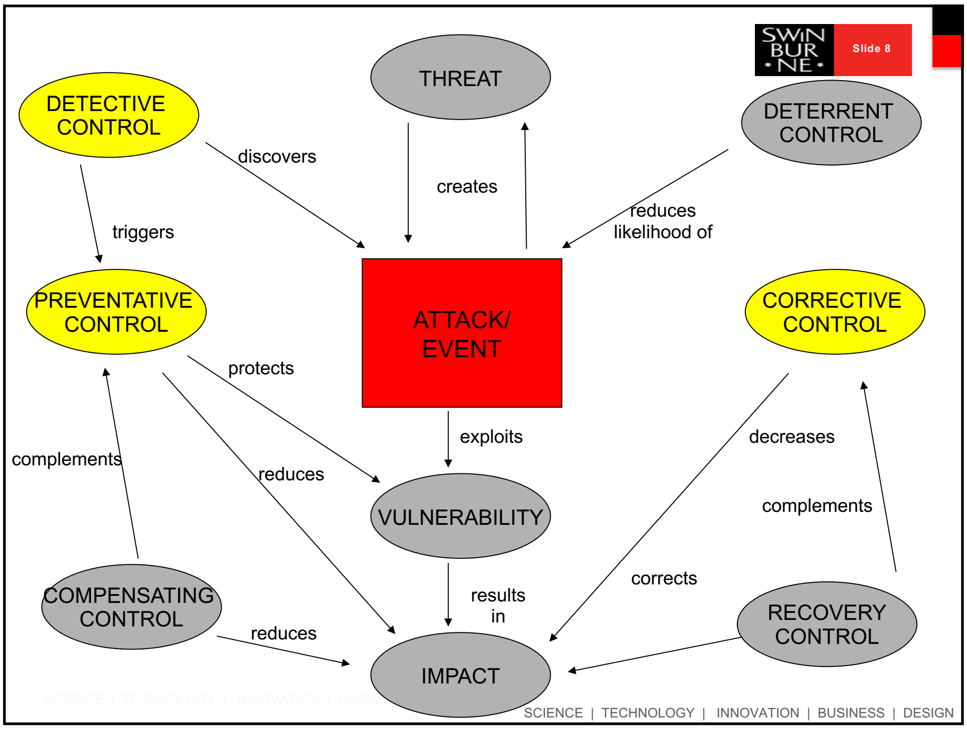
Control activities are the policies, procedures, techniques, and mechanisms that are applied to help ensure that the information assets identified as being at risk during a risk assessment are managed

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

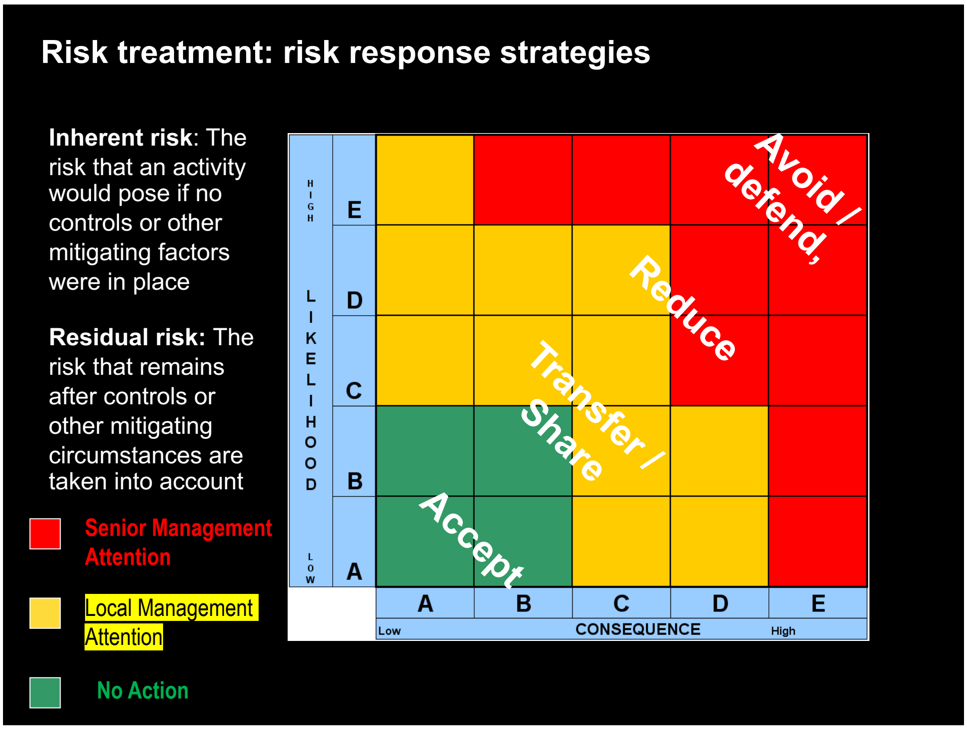
SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

7



SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

8



Risk treatment: risk response strategies

Inherent risk: The risk that an activity would pose if no controls or other mitigating factors were in place

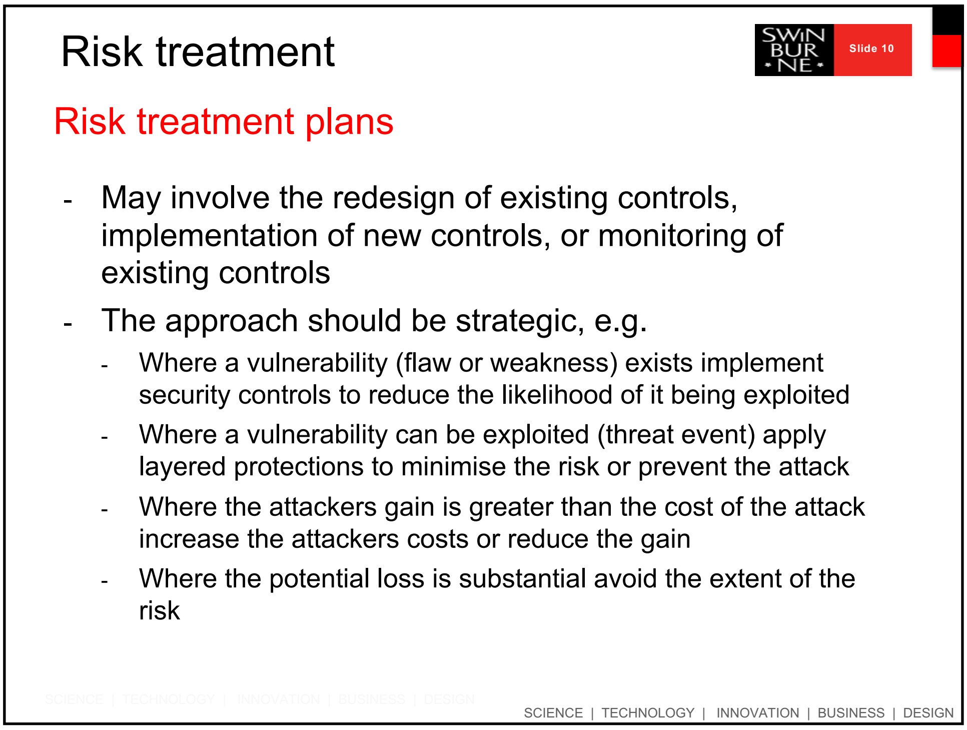
Residual risk: The risk that remains after controls or other mitigating circumstances are taken into account

🟥 Senior Management Attention

🟨 Local Management Attention

🟩 No Action

LIKELIHOOD		A	B	C	D	E
HIGH	E	🟨	🟥	🟥	🟥	🟥
	D	🟨	🟨	🟨	🟥	🟥
	C	🟨	🟨	🟨	🟥	🟥
	B	🟩	🟩	🟨	🟨	🟥
LOW	A	🟩	🟩	🟨	🟨	🟥

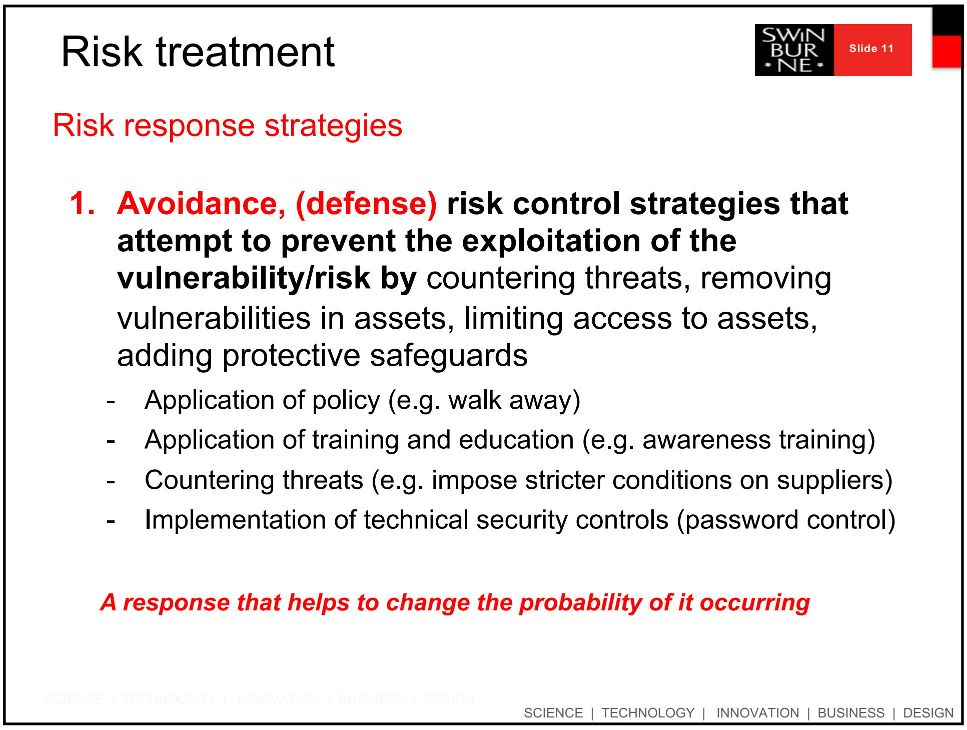


Risk treatment

Slide 10

Risk treatment plans

- May involve the redesign of existing controls, implementation of new controls, or monitoring of existing controls
- The approach should be strategic, e.g.
  - Where a vulnerability (flaw or weakness) exists implement security controls to reduce the likelihood of it being exploited
  - Where a vulnerability can be exploited (threat event) apply layered protections to minimise the risk or prevent the attack
  - Where the attackers gain is greater than the cost of the attack increase the attackers costs or reduce the gain
  - Where the potential loss is substantial avoid the extent of the risk



Risk treatment

SWIN BUR NE Slide 11

Risk response strategies

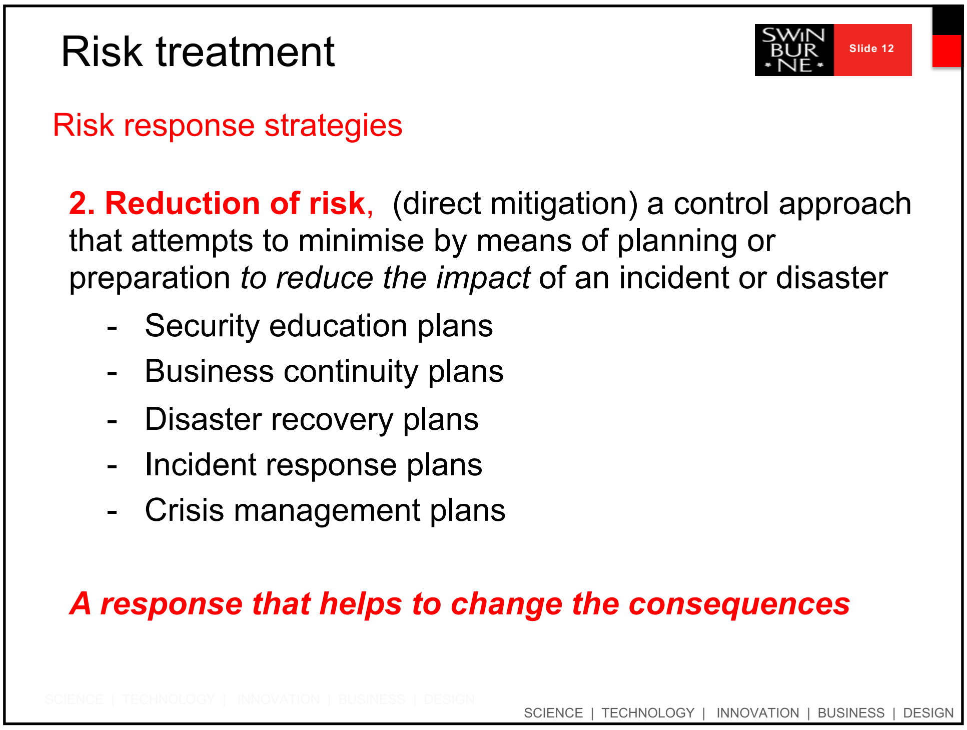
1. **Avoidance, (defense) risk control strategies that attempt to prevent the exploitation of the vulnerability/risk by** countering threats, removing vulnerabilities in assets, limiting access to assets, adding protective safeguards

- Application of policy (e.g. walk away)
- Application of training and education (e.g. awareness training)
- Countering threats (e.g. impose stricter conditions on suppliers)
- Implementation of technical security controls (password control)

A response that helps to change the probability of it occurring

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

11



Risk treatment

SWIN BUR NE Slide 12

Risk response strategies

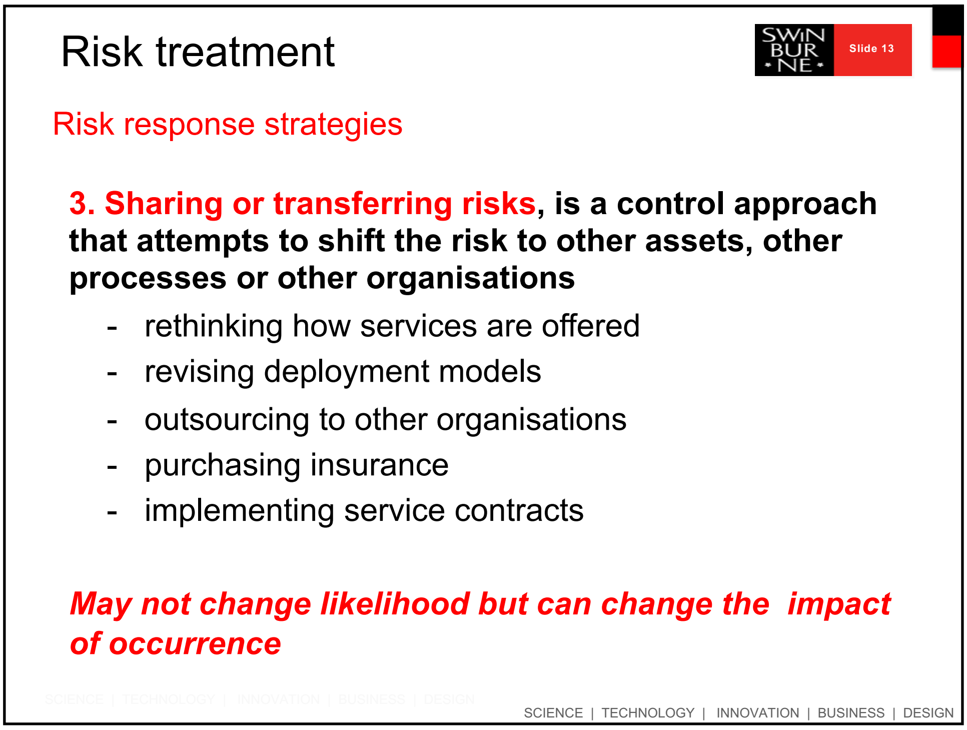
2. Reduction of risk, (direct mitigation) a control approach that attempts to minimise by means of planning or preparation *to reduce the impact* of an incident or disaster

- Security education plans
- Business continuity plans
- Disaster recovery plans
- Incident response plans
- Crisis management plans

A response that helps to change the consequences

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

12



Risk treatment

Slide 13

Risk response strategies

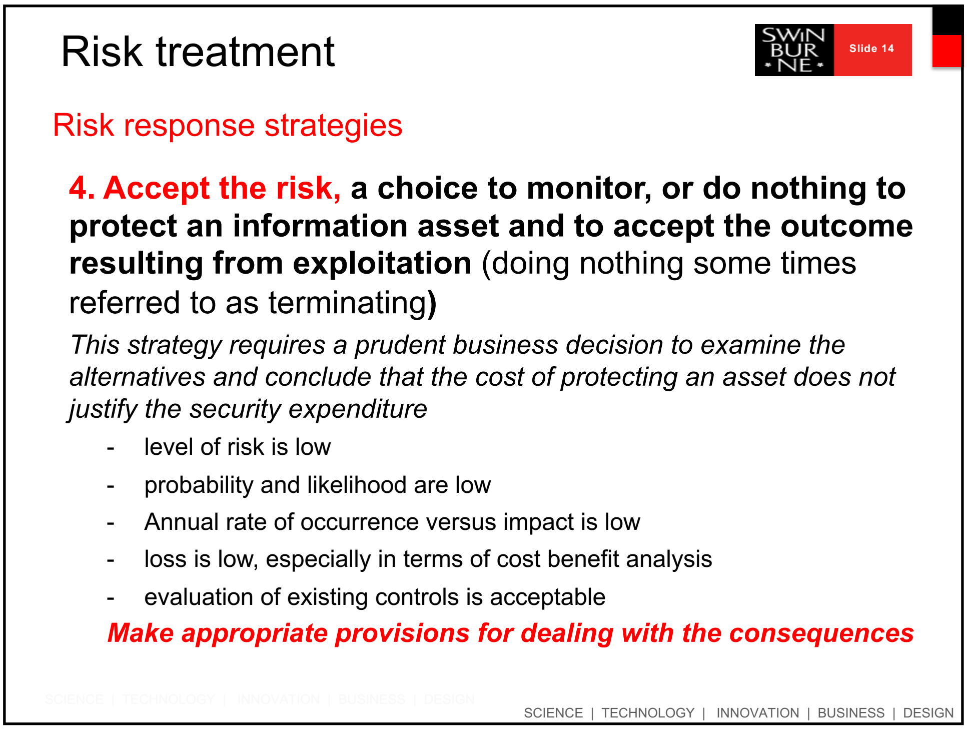
3. Sharing or transferring risks, is a control approach that attempts to shift the risk to other assets, other processes or other organisations

- rethinking how services are offered
- revising deployment models
- outsourcing to other organisations
- purchasing insurance
- implementing service contracts

May not change likelihood but can change the impact of occurrence

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

13



Risk treatment

Slide 14

Risk response strategies

4. Accept the risk, a choice to monitor, or do nothing to protect an information asset and to accept the outcome resulting from exploitation (doing nothing some times referred to as terminating**)**

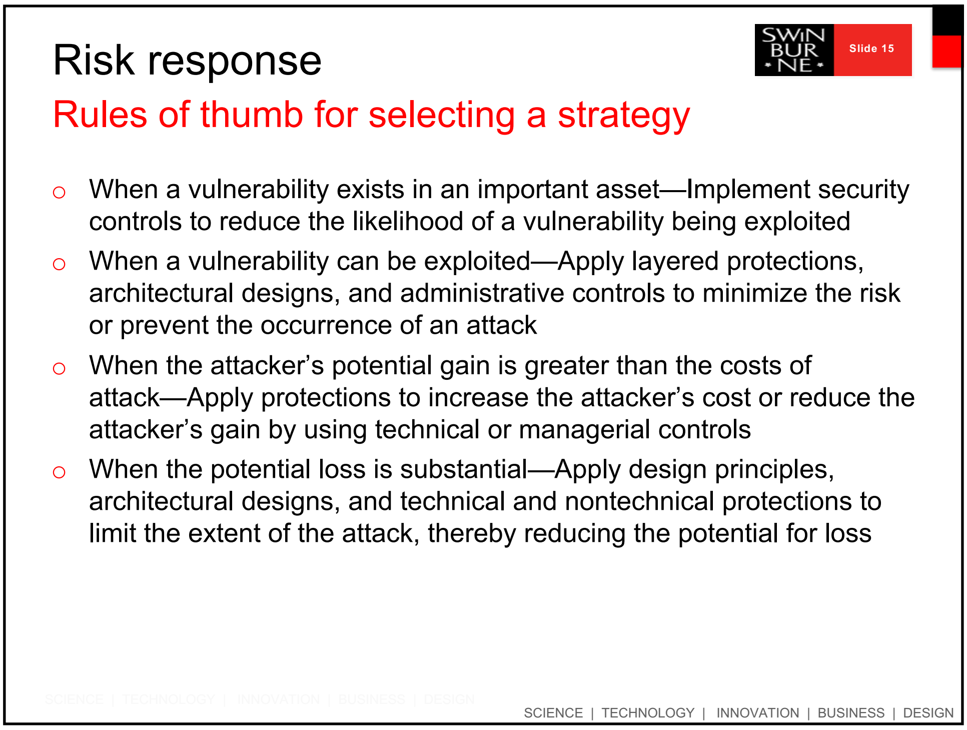
This strategy requires a prudent business decision to examine the alternatives and conclude that the cost of protecting an asset does not justify the security expenditure

- level of risk is low
- probability and likelihood are low
- Annual rate of occurrence versus impact is low
- loss is low, especially in terms of cost benefit analysis
- evaluation of existing controls is acceptable

Make appropriate provisions for dealing with the consequences

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

14



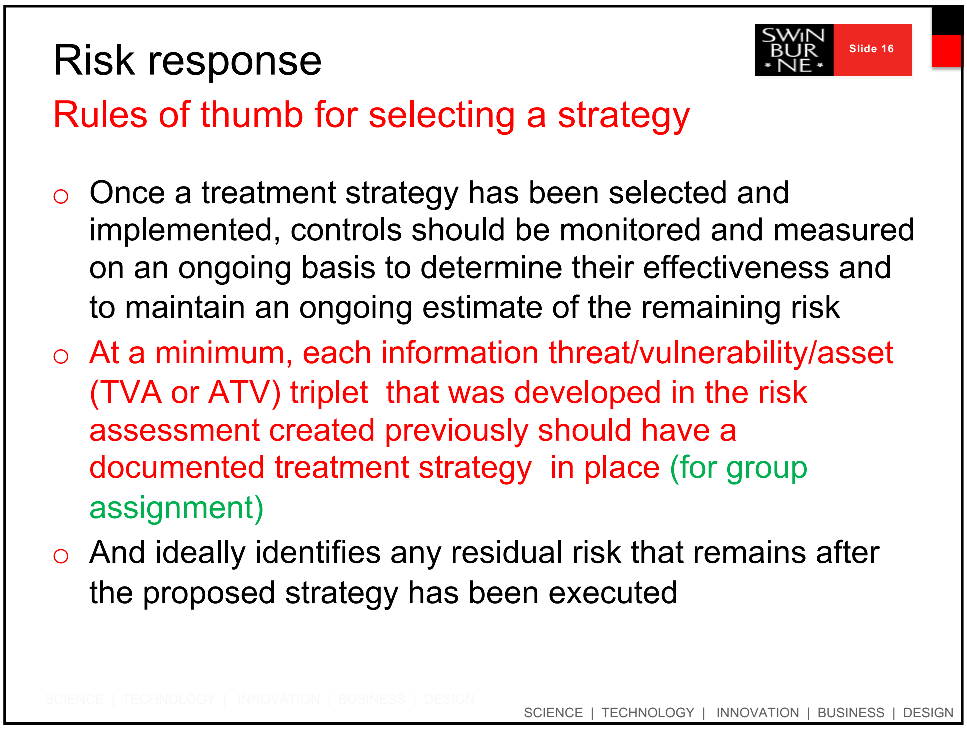
Slide 15

Risk response

Rules of thumb for selecting a strategy

- When a vulnerability exists in an important asset—Implement security controls to reduce the likelihood of a vulnerability being exploited
- When a vulnerability can be exploited—Apply layered protections, architectural designs, and administrative controls to minimize the risk or prevent the occurrence of an attack
- When the attacker's potential gain is greater than the costs of attack—Apply protections to increase the attacker's cost or reduce the attacker's gain by using technical or managerial controls
- When the potential loss is substantial—Apply design principles, architectural designs, and technical and nontechnical protections to limit the extent of the attack, thereby reducing the potential for loss

15



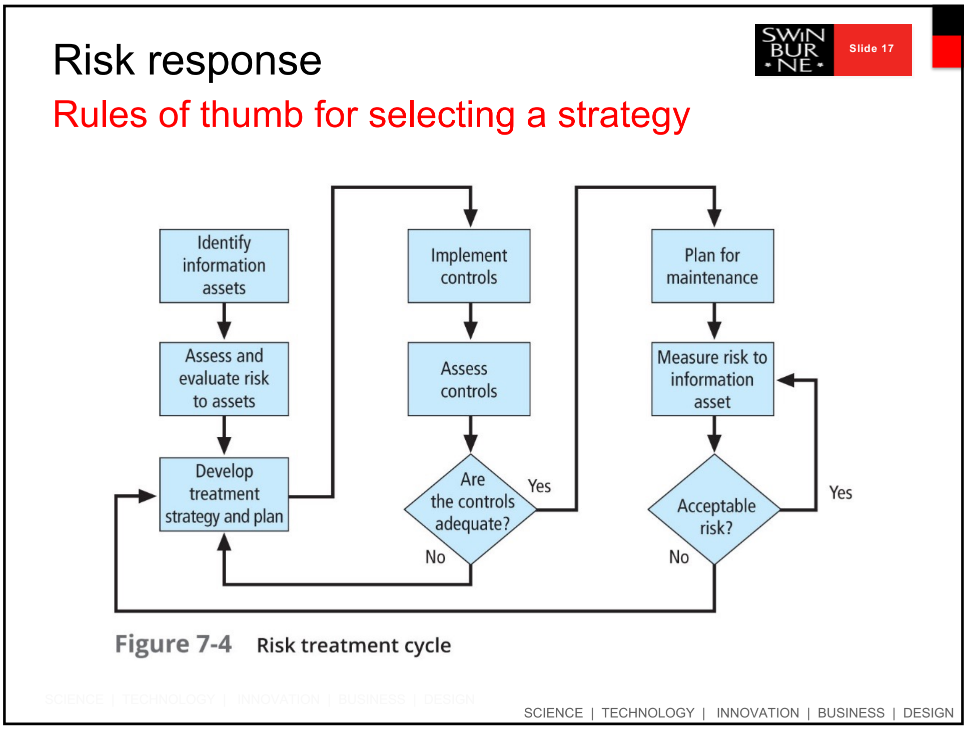
Slide 16

Risk response

Rules of thumb for selecting a strategy

- Once a treatment strategy has been selected and implemented, controls should be monitored and measured on an ongoing basis to determine their effectiveness and to maintain an ongoing estimate of the remaining risk
- At a minimum, each information threat/vulnerability/asset (TVA or ATV) triplet that was developed in the risk assessment created previously should have a documented treatment strategy in place (for group assignment)
- And ideally identifies any residual risk that remains after the proposed strategy has been executed

16



Risk response

Rules of thumb for selecting a strategy

Identify information assets

Assess and evaluate risk to assets

Develop treatment strategy and plan

Implement controls

Assess controls

Are the controls adequate?

Yes

No

Plan for maintenance

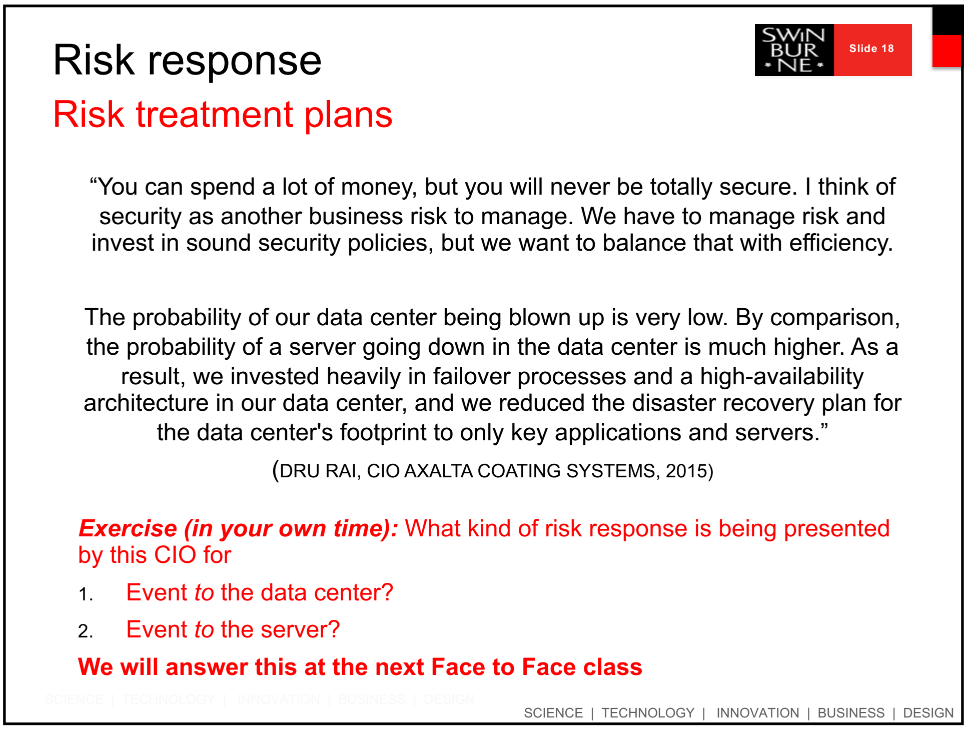
Measure risk to information asset

Acceptable risk?

Yes

No

Figure 7-4 Risk treatment cycle



Risk response

Risk treatment plans

"You can spend a lot of money, but you will never be totally secure. I think of security as another business risk to manage. We have to manage risk and invest in sound security policies, but we want to balance that with efficiency.

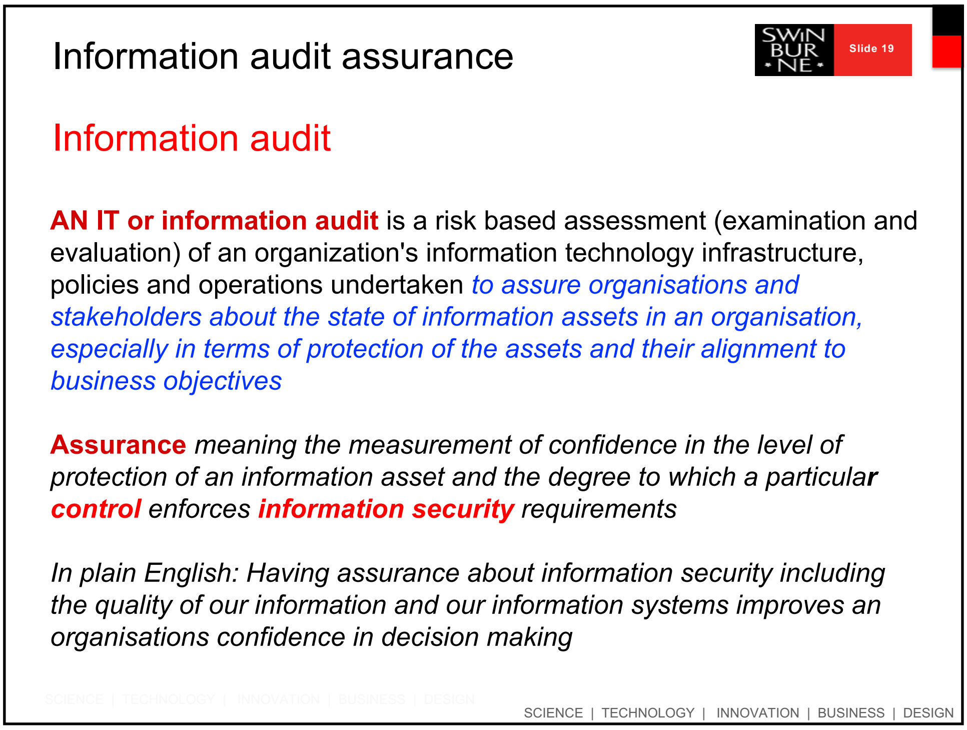
The probability of our data center being blown up is very low. By comparison, the probability of a server going down in the data center is much higher. As a result, we invested heavily in failover processes and a high-availability architecture in our data center, and we reduced the disaster recovery plan for the data center's footprint to only key applications and servers."

(DRU RAI, CIO AXALTA COATING SYSTEMS, 2015)

Exercise (in your own time): What kind of risk response is being presented by this CIO for

1. Event *to* the data center?
2. Event *to* the server?

We will answer this at the next Face to Face class



Information audit assurance

SWIN BUR NE Slide 19

Information audit

AN IT or information audit is a risk based assessment (examination and evaluation) of an organization's information technology infrastructure, policies and operations undertaken *to assure organisations and stakeholders about the state of information assets in an organisation, especially in terms of protection of the assets and their alignment to business objectives*

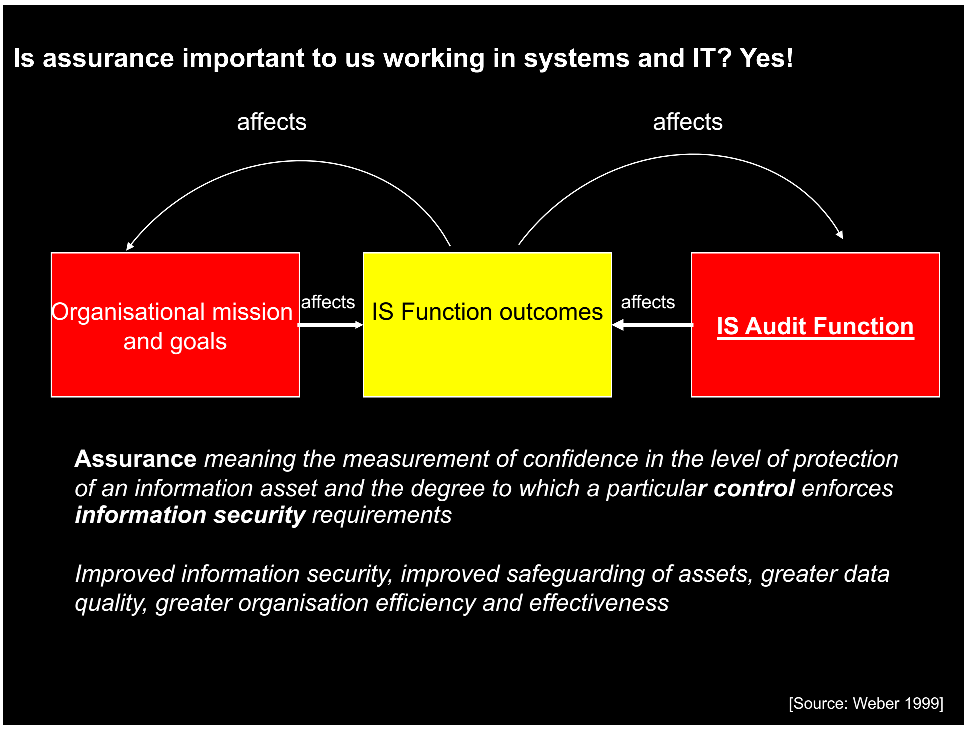
Assurance *meaning the measurement of confidence in the level of protection of an information asset and the degree to which a particular* ***control*** *enforces* ***information security*** *requirements*

In plain English: Having assurance about information security including the quality of our information and our information systems improves an organisations confidence in decision making

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

19



Is assurance important to us working in systems and IT? Yes!

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*** *requirements*

Improved information security, improved safeguarding of assets, greater data quality, greater organisation efficiency and effectiveness

[Source: Weber 1999]

20

Information audit and assurance

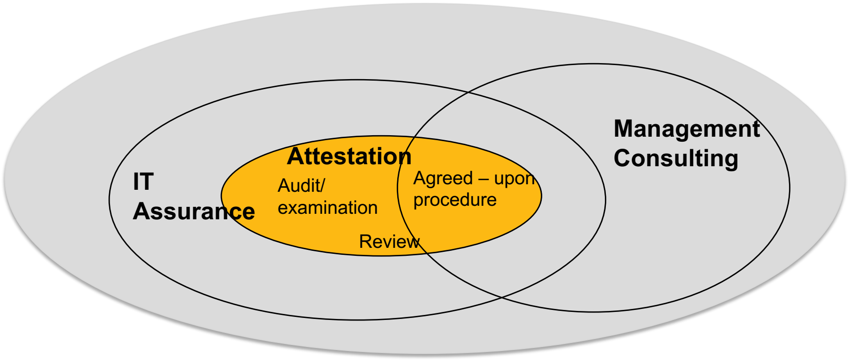
“The IT auditor should look for evidence of a prescribed, documented IT strategic planning process, because the existence of an ongoing process of this nature *indicates the company is diligently seeking an optimal fit between the information technology infrastructure and the organizations overall goals and objectives”*

Often viewed as the last defense in resolving corporate governance issues and the protection of organizational assets but, Information audit should be seen as the first step: a strategically placed tool that supports IT security management, good governance and adds value to the organization

[Source Hunton et al. Core Concepts in Information Technology Auditing 2004

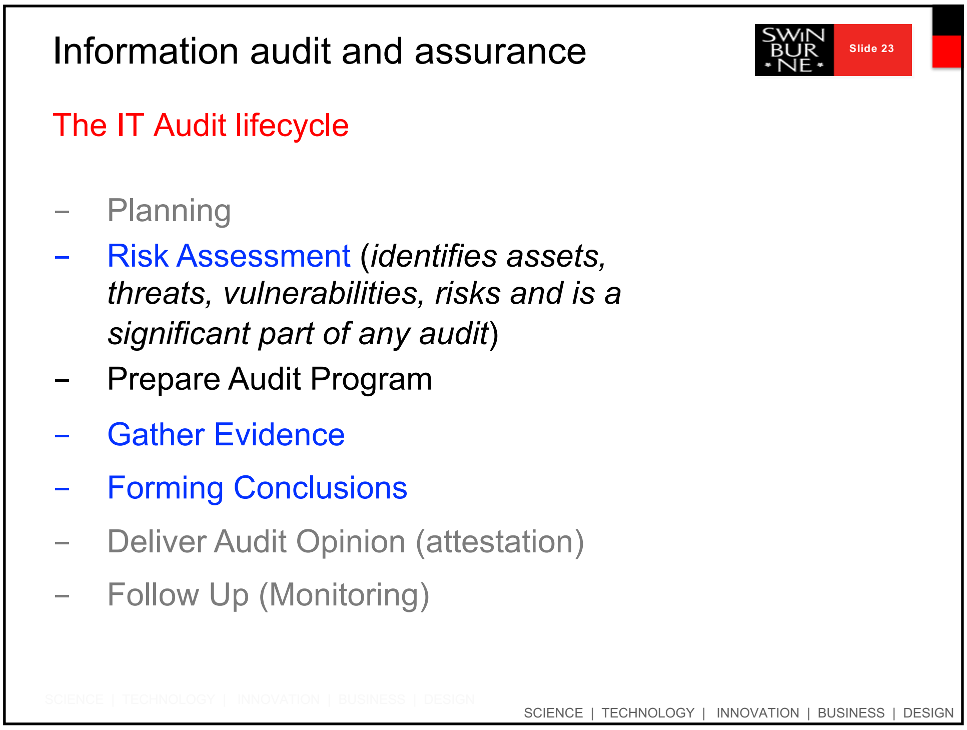
Information audit and assurance

Information Audit and assurance services



Attestation is the formal affirmation of the audit process: it is signed off as complete and accurate

[Source AICPA cf, Information Technology, Auditing and Assurance, Hall & Singleton 2005]



Information audit and assurance

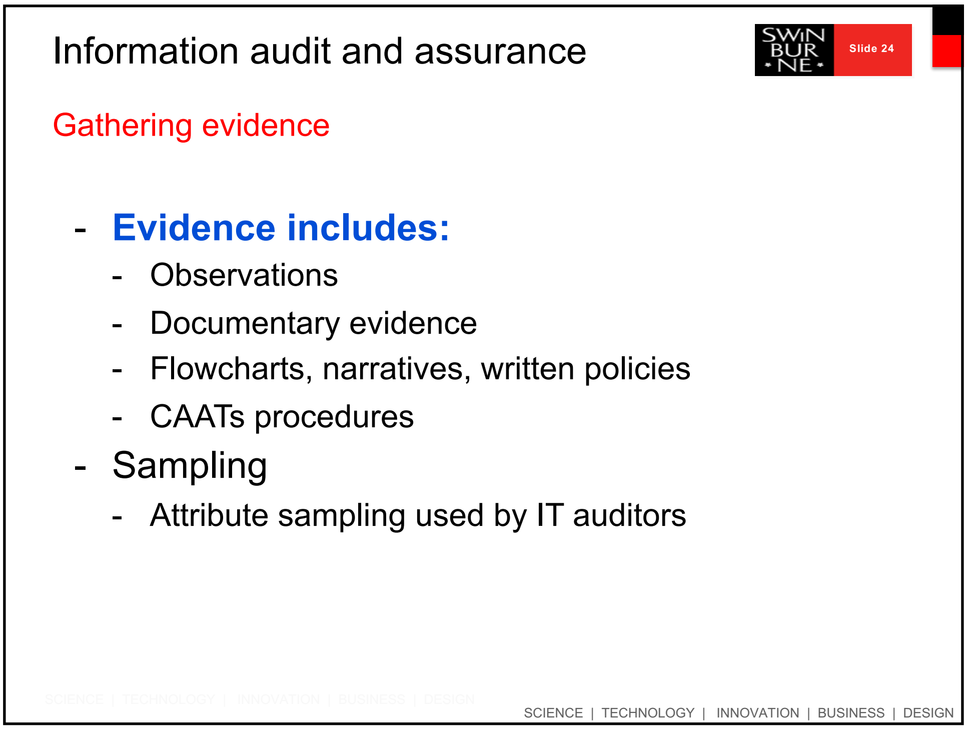
Slide 23

The IT Audit lifecycle

- Planning
- Risk Assessment (*identifies assets, threats, vulnerabilities, risks and is a significant part of any audit*)
- Prepare Audit Program
- Gather Evidence
- Forming Conclusions
- Deliver Audit Opinion (attestation)
- Follow Up (Monitoring)

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

23



Information audit and assurance

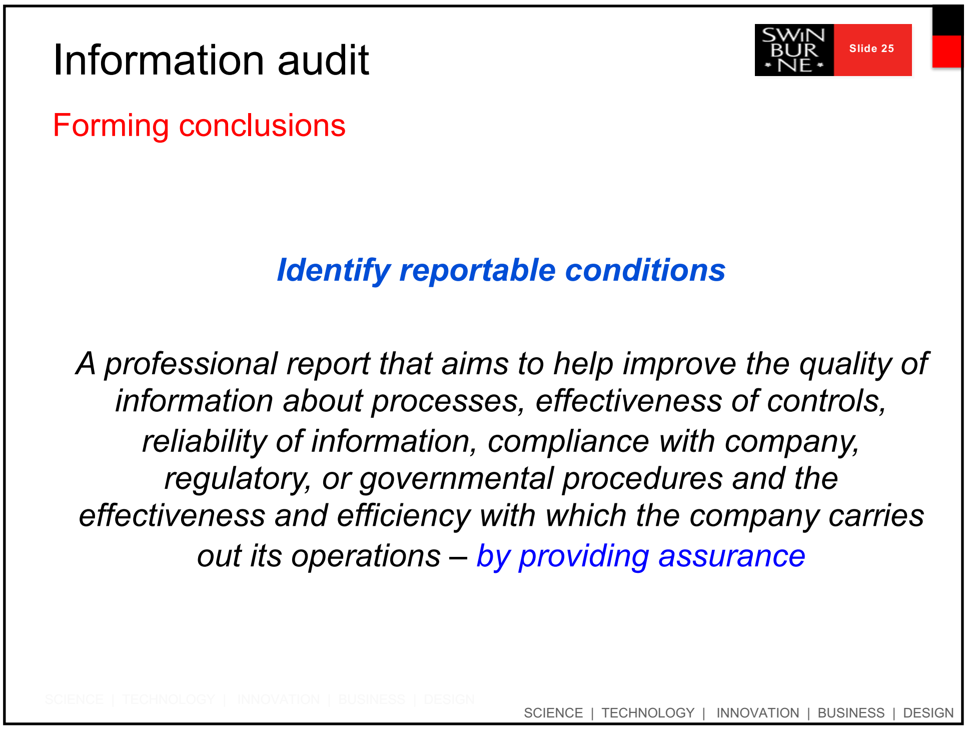
Slide 24

Gathering evidence

- **Evidence includes:**
  - Observations
  - Documentary evidence
  - Flowcharts, narratives, written policies
  - CAATs procedures
- Sampling
  - Attribute sampling used by IT auditors

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

24

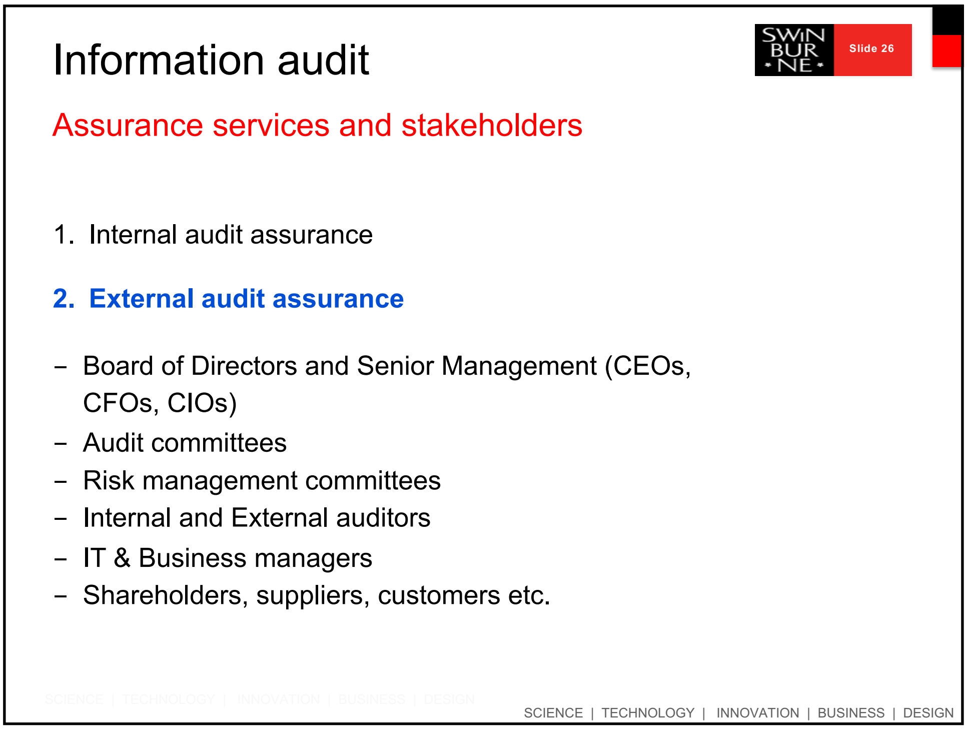


Information audit

Forming conclusions

Identify reportable conditions

A professional report that aims to help improve the quality of information about processes, effectiveness of controls, reliability of information, compliance with company, regulatory, or governmental procedures and the effectiveness and efficiency with which the company carries out its operations – by providing assurance



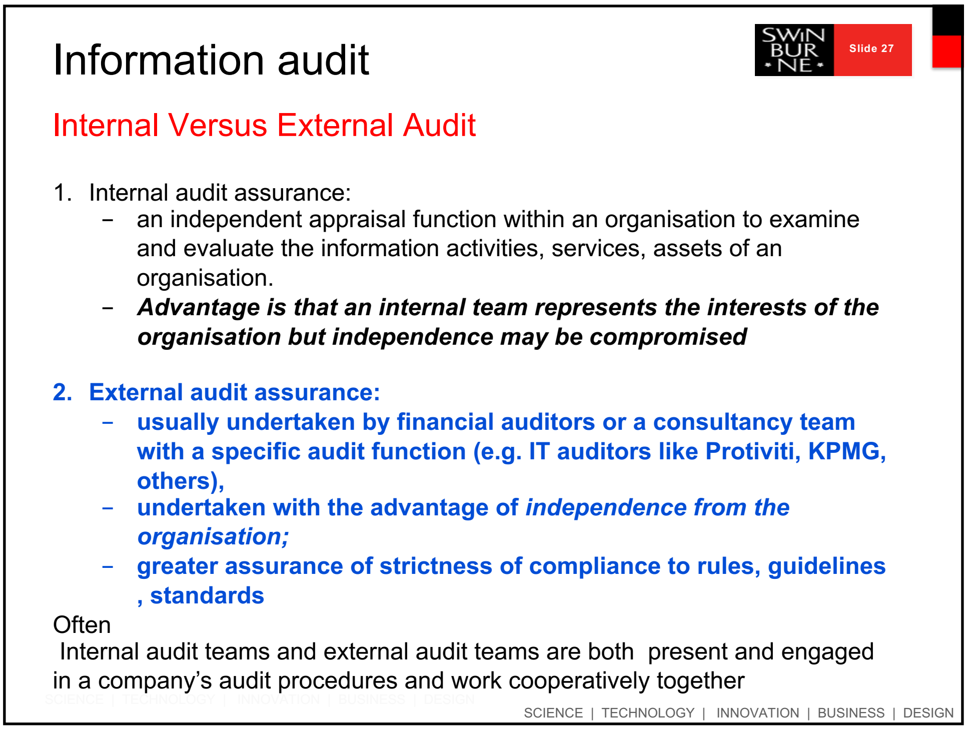
Information audit

Assurance services and stakeholders

1. Internal audit assurance

2. **External audit assurance**

- Board of Directors and Senior Management (CEOs, CFOs, CIOs)
- Audit committees
- Risk management committees
- Internal and External auditors
- IT & Business managers
- Shareholders, suppliers, customers etc.



Information audit

Slide 27

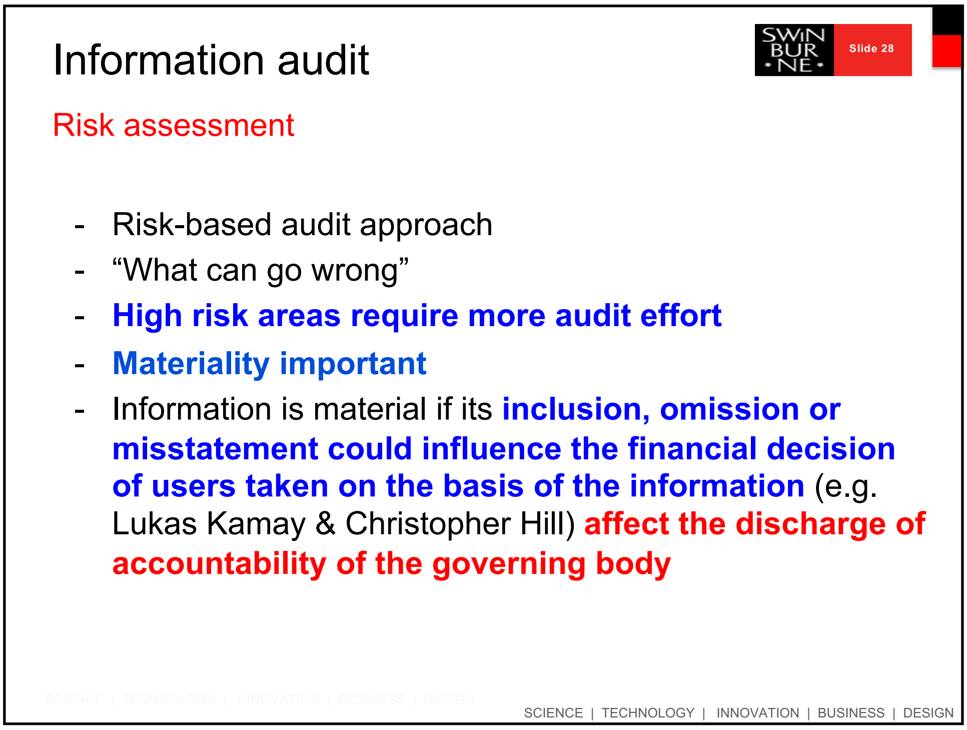
Internal Versus External Audit

1. Internal audit assurance:
   - an independent appraisal function within an organisation to examine and evaluate the information activities, services, assets of an organisation.
   - ***Advantage is that an internal team represents the interests of the organisation but independence may be compromised***

2. **External audit assurance:**
   - **usually undertaken by financial auditors or a consultancy team with a specific audit function (e.g. IT auditors like Protiviti, KPMG, others),**
   - **undertaken with the advantage of *independence from the organisation;***
   - **greater assurance of strictness of compliance to rules, guidelines , standards**

Often
Internal audit teams and external audit teams are both present and engaged in a company's audit procedures and work cooperatively together

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN



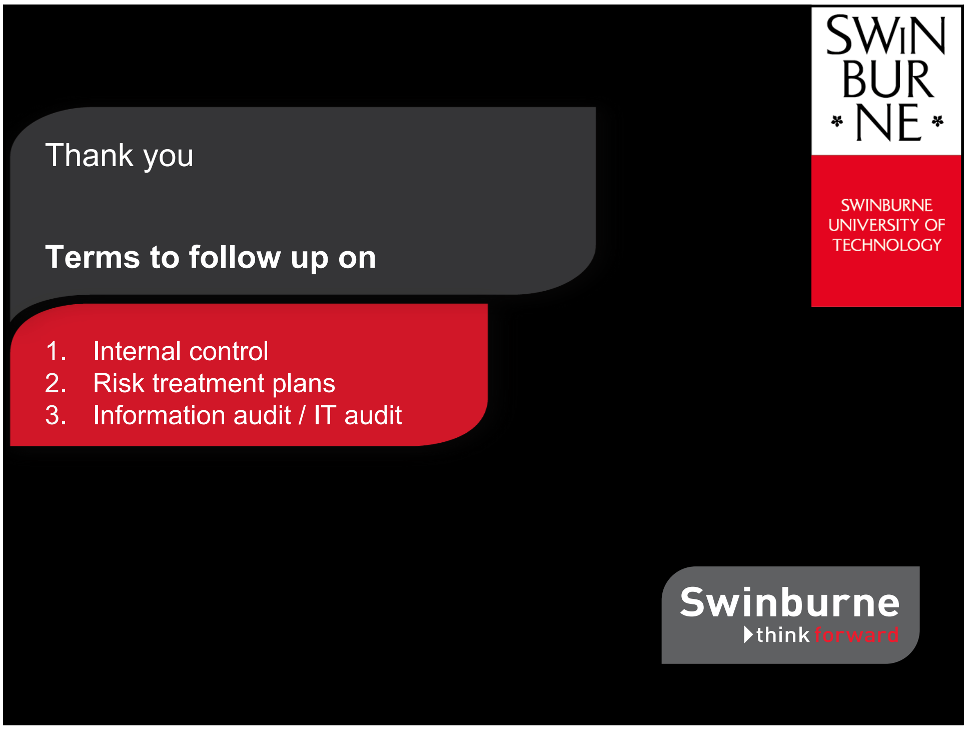
Information audit

Slide 28

Risk assessment

- Risk-based audit approach
- "What can go wrong"
- **High risk areas require more audit effort**
- **Materiality important**
- Information is material if its **inclusion, omission or misstatement could influence the financial decision of users taken on the basis of the information** (e.g. Lukas Kamay & Christopher Hill) **affect the discharge of accountability of the governing body**

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN



Thank you

Terms to follow up on

1. Internal control
2. Risk treatment plans
3. Information audit / IT audit