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 – M007 completed

Assessments

- CLA#1 , CLA#2 submitted and returned marking, CLA#3 in process
- Group warm up exercise completed (*those present receive mark*)
- Quiz 1 completed. Quiz 2 in week 12

Groups

- Group registration concluded in weeks 7
- Group assignment due Friday 21 October

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

2

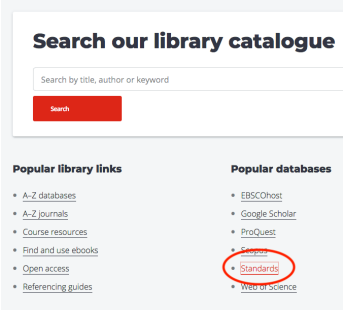
Reading for this week's topic

Unit texts:

- **Whitman, Michael E. annd Mattord, Herbert J. Chapter 10 Planning for Contingencies. *Management of information security*. Sixth Edition., Stamford, Conn. : Cengage Learning, 2019.**
- Gibson, Darril, Chapters 11-13. Chapter 11, Turning your Risk Assessment into a Risk Mitigation Plan, Chapter 12, Mitigating Risk with a Business Impact Analysis, Chapter 13, Mitigating Risk with a Business Continuity Plan, *Managing Risk in Information Systems*. 2015.

Additional reading list

- HB292-2006 – (A Practitioners Guide to
- Business Continuity Management ,
- Swinburne Library SAI Database)
- Gibson Chapters 11- 15
- Whitman Chapters 7, 10



3

Business continuity management

BCM Standards and guidelines (ISO 22301: 2019)

HB292-2006 – (A Practitioners Guide to Business Continuity Management , Swinburne Library SAI Database)

NIST800-34 Rev.1 - Contingency Planning Guide for Federal Information Systems (available online)

The Auditor-General ANAO Report No.6 2014–15 Performance Audit: Business Continuity Management https://www.anao.gov.au/work/performance-audit/business-continuity-management **(recommended unit reading)**

AS ISO 22313:2017, Societal security—Business continuity management systems—Guidance

SA TS ISO 22317:2017, Societal security—Business continuity management systems—Guidelines for business impact analysis (BIA)

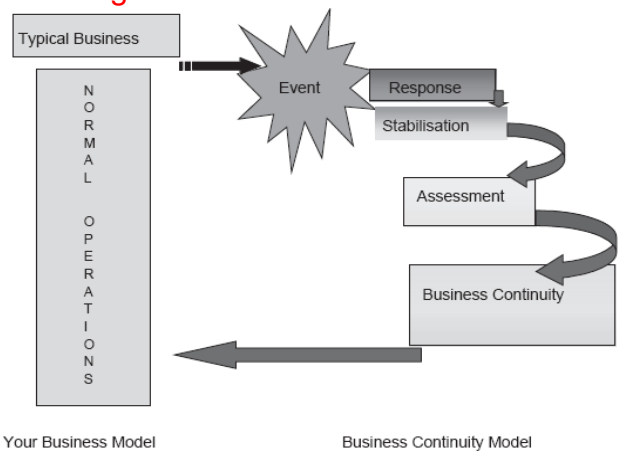
ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements

4

Incidents, disasters and response

Slide 5

BCM is all about response not recovery - Maintaining business through a crisis



5

This week's learning plan

Slide 6

Gain an understanding of

1. Understanding the strategic significance of business resilience
2. Understanding of the role of disruption scenarios in BCM and contingency planning
3. Appreciate the importance of business impact analysis for BCM and contingency planning
4. Understand the role of stakeholder analysis and communication planning in BCM
5. *Next week Incident Response Planning*

6

Your group assignment

Slide 7

A deep dive on BCM

Identify further opportunities of work in the risk management and information security management area, prioritising business continuity and incident response associated with risks to information assets you have identified and how eTricity should address them

The assignment can be considered in two halves

Items 1 - 2

- BCM planning inclusive of Information Governance, Information Security Policy & Information Security-Risk mitigation for 5 priorities (avoid, share, reduce, accept)

Items 3 - 4

- Advising eTricity on the need for a business continuity through BIA, prioritized business impact assessments, with parameters for response
- A brief Incident Response Plan (IRP) inclusive of communications planning as part of this

7

BCM and contingency planning

Slide 8

What does this model tell us about resilience?

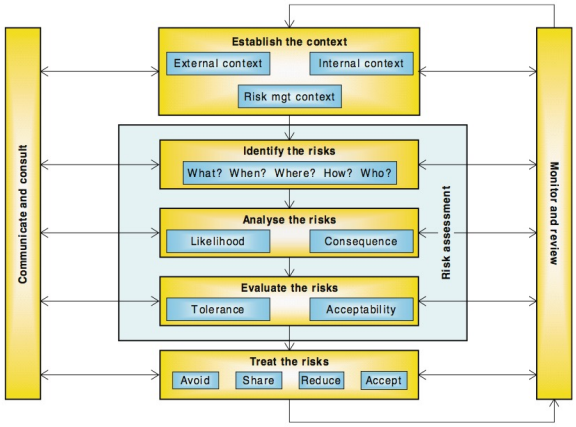


FIGURE 6 THE RISK MANAGEMENT PROCESS*

* based on AS/NZS 4360:2004

8

BCM and contingency planning

Slide 9

Resilience

- The goal of resilient organisation is to continue critical operations (business/mission essential services) at all times, during any disruption – without excessive interruption
- This is not a process –its an end state: The ability to resist, absorb & recover from adversity or a change a conditions, including successfully adapting
- The process is the work that is done to adapt to change and manage risks to minimise adverse affects on critical business functions
- i.e. you build resilience - its about agility, risk management, continuity and contingency management

NIST800-34, Contingency Planning Guide for Federal Information Systems

9

BCM and contingency planning

Slide 10

Resilience

- A strategic benefit of BCM should be improved operational resilience to unforseen events
- Continuity *planning* & contingency *planning*- continuity the ability to continue business Vs contingency those plans that are about recovering services through one plan or another
- A strategic benefit of BCM should be improved operational resilience to unforseen events
- But its not just a BCP view, Risk management as we have prepared it proactively enhances the resilience of an organisation in the event of future disruption

  e.g. through the “resilience” of security systems, back-up systems, off-site storage and arrangements including communication strategies and HR training ..and *planned mitigation strategies*

10

BCM and contingency planning

Slide 11

Resilience is the *context & attitude* (appetite?) of BCM

"Resilient entities continue to meet organisational objectives when faced by major challenges such as natural disasters, crime, equipment failures or even terrorist attack. **Resilience takes a holistic approach** to help entities survive turbulent times, by integrating risk, emergency response, incident and business continuity management. Resilience arises from a combination of culture and attitude, process and framework."

ANAO- BCM

"**Resilient organizations continually work to adapt to changes and risks that can affect their ability to sustain operations.** Risk management, contingency, and continuity planning are individual security and emergency management activities that can be implemented **in a holistic manner** across an organization as components of a resiliency program."

NIST800-34

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

11

BCM and disruption scenarios

Slide 12

Analysing the consequences of disruption

- Risk assessment helps us identify and prioritises risks, threats, vulnerabilities to information assets and an organisation's resources, …..especially those that are business critical, then
- It is possible to develop scenarios for potential disruptions to an organisations business critical processes and from that a clearer understanding of their impact on a business
- This way rather than developing a response to every identified risk we can develop strategies to respond to the scenario

  e.g. a fire in the Dandenong ranges threatening the data centre, an industrial dispute and strikers barricade at the data centre could all result in the same disruption scenario: *"loss of access to building for greater than 24 hours"*

- In this case we can plan business continuity for the consolidated scenario rather rather than 2 or more separate risks

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

12

BCM and disruption scenarios

Slide 13

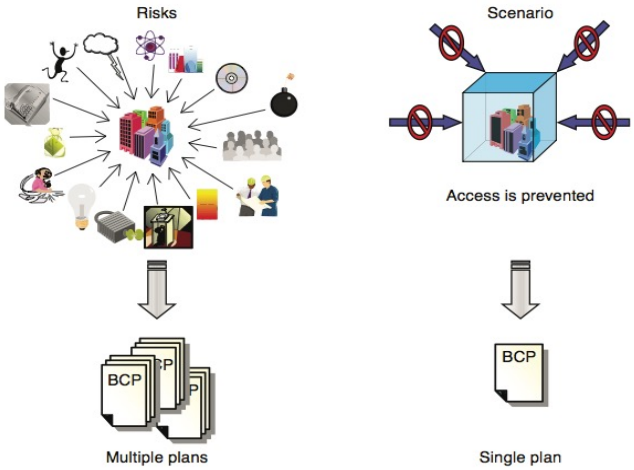


FIGURE 11 ALIGNING RISKS IN SCENARIOS

13

BCM and disruption scenarios

Slide 14

3.13 Risk assessment templates

Identify potential disruption causes and contributing factors

Determine the overall consolidated risk or risk scenario

Determine the level of risk from the consequence and likelihood

Identify vulnerabilities to the risk existing in people, property, information, or processes.

Identify gaps in current controls or treatments that need to be addressed

Template 3.1
Disruption risk register

Risk sources (What are the potential causes and contributing factors)	Risk (including detailed description of the risk)	Overall disruption risk/ Risk scenario	Risk assessment: Consequence	Risk assessment: Likelihood	Risk assessment: Risk rating	Existing controls or strategies	Vulnerabilities	Treatments: Being Developed	Treatments: Need to be developed	Responsibility
Loss of external power. Damage to supply infrastructure. Building cabling/power control, failure.	**Power loss** Loss of power supply results in loss of: lifts, A/C systems and building access control for a period of greater than eight hours.	Loss of building access	Major	Possible	High	Back up generator on auto switch, capacity for critical floors only	Ageing electrical infrastructure within building. Floors 1 to 11 without backup power supply. No alternate site arrangements.	Mutual aid agreement with Acme organisation for use of 10 seats	Upgraded back up generator to provide power to 30% more of operation	GM Corporate Services.

Describe the risk with its associated impacts

Assess the consequence should the disruption occur

Assess the likelihood of a disruption with that consequence thoccurring with that consequence

Describe existing controls or strategies that would mitigate the risk

Describe treatments commenced but not yet not yet implemented

Identify the person/ position responsible for the risk & its treatment(s)

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

14

BCM , disruption scenarios & BIA

Slide 15

Your information risk assessment will have identified a lot of significant business processes (*critical business functions & impact on operations*), it is necessary to distill these down into a prioritised list of the critical processes. That is, those processes that must be performed in order to enable the entity to meet its most important objectives (mission critical).

Identify locations impacted or included within the scope of the assessment

Describe the key overall impacts on each critical business function

Determine requirement for an update or development of new BCP

Template 3.2
Disruption scenario register

Overall disruption risk/ risk scenario *(obtained from Column 3 of Risk & Vulnerability Register)*	Location(s) *(where specific sites are involved)*	Critical business function	Impact on business operations *(describe the overall impact to the successful operation of your business and the key business functions affected)*	BCP status	
				Current	Required
Loss of access to IT systems	Level 8, North Tower, Capital City	Financial transactions	Transaction cannot proceed without access to financial data. Accounts payable, accounts receivable and financial reporting cannot proceed. Integrity of financial data may be compromised	✓ 8 Jan 2005	✓ Update

Determine Critical Business functions at each location

Identify if a current BCP is in place and the date of its last update

15

BCM and contingency planning

Slide 16

Business Impact Analysis (BIA)

- A BIA determines *the impact that a disruption event could have on businesses operations*. And, what we are most interested in is the impact on *critical* business *operations* process.
- *Then*, what is the impact on the activities and resources that support those critical business processes ….so that a response can be planned
- For the **critical processes (i.e. 4-5 major/critical business functions – risk areas - in your planning) you** identified and distilled through scenario analysis (to approx 3-4 major scenarios), need to consider
  - a list of the activities and resources crucial to that critical business function; (e.g. Sales > online shop > and web servers)
  - interdependencies within and between internal activities and resources OR interdependencies with and between external entities;
  - a priority ranking of the processes, activities and resources which represents the entity's agreed view.

16

Business Impact Analysis

HB292-2006

A Practitioners Guide to Business Continuity Management

Some QLD Gov't resources

https://www.youtube.com/watch?v=em-A_HSQNns&feature=youtu.be

https://www.business.qld.gov.au/business/running/risk-management/risk-management-plan-business-impact-analysis/conduct-business-impact-anaylsis

57

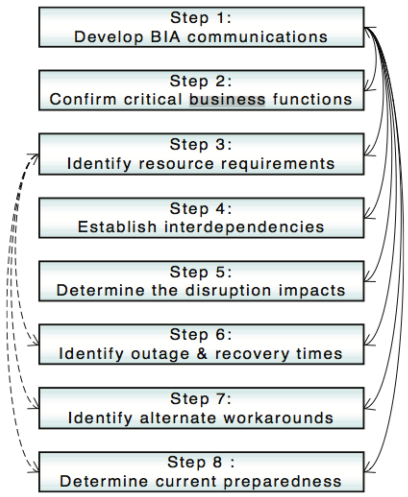
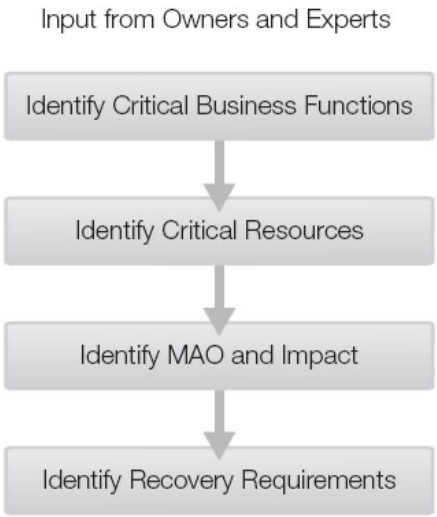


FIGURE 12 THE BUSINESS IMPACT ASSESSMENT PROCESS
(dotted lines represent information flows)

Be succinct, develop in tables with supporting analysis

17

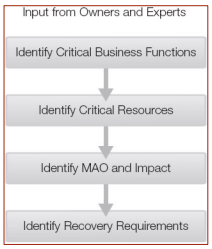
Business Impact Analysis involves…..



Gibson, Darril, *Managing Risk in Information Systems*. Jones & Bartlett Learning, Burlington, MA, U.S.A., 2015, Chapter 12: Mitigating Risk with a Business Impact Analysis

18

Our continuity planning involves (at assignment items 3…..)



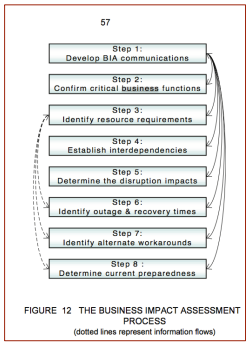


FIGURE 12 THE BUSINESS IMPACT ASSESSMENT PROCESS
(dotted lines represent information flows)

Undertake preliminary business continuity planning for our company by preparing

- a detailed business impact analysis for ***4-6 (5)*** prioritised risk areas (critical business functions, aligned to critical information assets)
- provide company with an explanation of the importance of the priorities you have chosen you have chosen,
- your BIA must include disruption scenarios for four approximately (3-4) prioritised business impact assessments.
- the recovery parameters for each of the four (4) priorities
- A general explanation of how this work supports contingency planning for your BCP modelling (steps i-iv). Include account of strategic importance of BCM and strategy for communications management in the event of a disaster within your general approach to BCP.

- We don't expect step 3, 4, 7 of HB292 to be covered in any great detail - step 8 goes to recovery (also covered by Gibson)

19

BCM and contingency planning

Business Impact Analysis

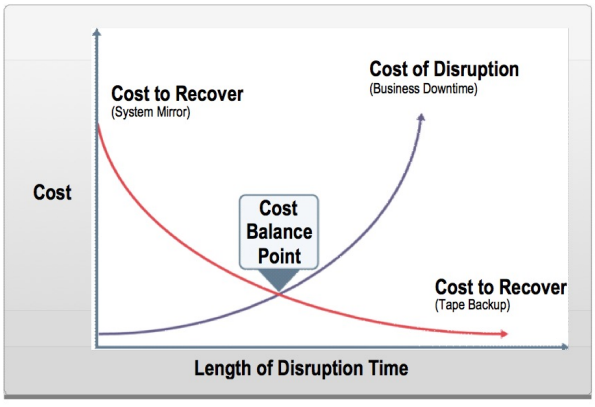


Figure 3-3: Cost Balancing

20

BCM and contingency planning: disruption impacts

Building qualitative measures, that extend the descriptive approach you have used in risk assessment is a good approach

Table 8
Measuring financial impacts of a disruption scenario (example only)

Rating	Category	Description
1	Insignificant	Financial loss <1% budget
2	Minor	Financial loss 1-5% budget
3	Moderate	Financial loss 5-25% budget
4	Major	Financial loss 25-30% budget
5	Catastrophic	Financial loss >30% budget

Table 9
Measuring operational (non-financial) impacts of a disruption scenario (example only)

Rating	Category	Description
1	Insignificant	No measurable operational impact to the business.
2	Minor	Minor degradation of service, impact limited to a single area of the business, management intervention required.
3	Moderate	Substantial degradation of service, impact to multiple areas of the business, can be managed with substantial management intervention and possible outside assistance.
4	Major	Significant degradation of service, impact to multiple areas of the business, threatens the viability of the enterprise, and requires significant mobilisation of resources and significant management intervention including external assistance.
5	Catastrophic	Threatens the immediate viability of the enterprise and introduces significant long term doubt on the viability of the enterprise. Immediate action required to minimise or mitigate the effect on most parts of the enterprise.

21

BCM and contingency planning

Business Impact Analysis: recovery metrics

- Need to assess the MTD/MAO – *maximum tolerable downtime* or *period of disruption*, i.e., how long can the critical business function survive without the activity/resource available to it before there is a detrimental effect? E.g. how long can we survivine without servicing our clients?
  also known as Maximum allowable outage
- Need to assess the RTO – recovery time objective - maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources. It is the maximum amount of time that an organisation sets for the recovery of critical requirements

  Essentially the RTO must ensure that the MTD and MAO are not exceeded
- Might distinguish from the RPO – recovery point objective – the time set for full recovery of systems, data and operations

22

BCM and contingency planning

Slide 23

Business Impact Analysis

Critical business process <insert process name>- details

Critical Business Process: <insert process name>	
Process description	
Process frequency	
Critical periods	
Key contacts	
Maximum tolerable period of disruption	
Manual workarounds description	

But what is missing? No RTO/RPO provided, no link back to scenario-
undertake some research and decide a model

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

23

What is stakeholder management?

Slide 24

Is Stakeholder management a crucial part of the Group assignment?

- One of the most critical aspects of risk management and in running BCM programs is knowing who is important - what are peoples' relationships to internal controls, who is most critical and who or what individual/roles will impact (or be impacted) in a disruption to business operations.
- It is vital that stakeholder management, communications plans, crisis communications plans are developed to support BCM, coordinate responses, Gather input, check validity of information, Assign responsibilities, Increase awareness
- It is about successfully identifying stakeholders, analyzing their influence on the organization , and developing strategies to communicate, set boundaries, and managing (sometimes competing) expectations.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

24

Stakeholder Analysis

Slide 25

Identifying Stakeholders

- A stakeholder is any person, or organization (internal or external) that is actively involved in the business activity, or whose interests may be positively or negatively affected by a change or disruption to the activity – wider then just the owners and emloyees
- A stakeholder may also exert influence over the business activity If you are unsure, ask yourself who contributes and who will be affected by it?
- Think of an entire business activity for contributors, or the organization's political climate for potential impacts, and don't forget to consider external partners.
- Work with business units to identify all potential stakeholders.
- Interview key participants to help you uncover more stakeholders.

Stakeholder Analysis

Slide 26

Conduct a Stakeholder Analysis

3 key steps:

- Identify the relevant information for each stakeholder: relevant information are things like their particular interest in the business activity, their role in the activity, their level of authority (position), needs, and expectations
- Identify the potential impact or support of each stakeholder: this can be simple like using two measures low and high.
- Assess how key stakeholders are likely to react to various situations/ assess the sensitivity: another measure like low sensitivity or high sensitivity

Stakeholder Analysis

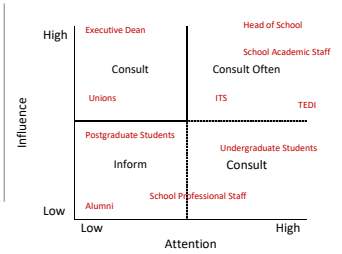
Slide 27

Conduct a Stakeholder Analysis

Your analysis can be plotted into a 2x2 grid that shows the stakeholder's relationship to the activity. This helps categorize stakeholders and determine where project management should direct its efforts. It is also a key input into the communications for risk management and scope planning.

Example adapted from:

University of Queensland *Guide for Leading Organisational Change, Stakeholder Analysis & Communication Plan retrieved 25 September 2015. http://www.uq.edu.au/search/index_nojs.php?q=stakeholder+analysis+and+communication+plan*



Mapping Influence and Attention

Stakeholder Analysis

Slide 28

Conduct a Stakeholder Analysis

Stakeholder group	Goals, motivations, and interests	Influence	Interest	Action	Win/win strategies
Senior Management Board	The successful delivery of the project on budget and on time.	High	High	Key player	Sign off of key decisions and stages via existing channels.
External Relations Office/Communications Office	Maintaining a positive public image for the university, its staff and students.	High	High	Key player	Partner in the development and delivery of the communication plan.
Catering Maintenance Cleaning	Ability to continue business as usual and potential impact on existing contracts.	Low	High	Show consideration	Show consideration via regular updates and provide clear channels for expressing concerns.
Fire service	Compliance with regulations and fire safety.	High	Low	Meet requirements	Ensure all projects follow correct procedures. No additional action.

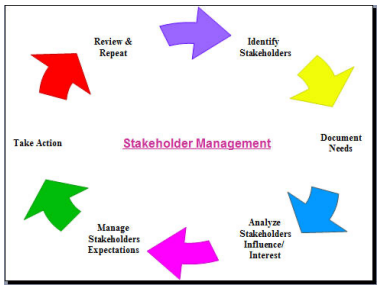
Stakeholder Analysis

Slide 29

Manage Stakeholders

In discussing these issues with risk managers, there are 2 questions:

1. what is the (crisis) communications plan (how is information shared)?
2. what is your project governance structure around stakeholders (how do people plug in, decisions get made, issues get escalated)?



SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

29

Stakeholder Analysis

Slide 30

Developing a communication map

- The goal of a successful communications approach is to manage expectations and minimize surprises. *Think about what the key message is and how to communicate it.*
- Manage the information that people get, their perceptions, and clarify the kind of feedback that you need in order to be effective in delivering the project.
- **A communications map** or matrix supports planning by taking the stakeholder analysis and identifying for each stakeholder or stakeholder group (**stakeholder**), the role that the stakeholder plays on the project **(role or responsibility**), what must be communicated (**the key message**), when (**how often / frequency**), how (**format/ channel of communication**) and whether a response is required and or status (**status**). At minimum, regular progress reports should be distributed to a wide audience.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

30

Stakeholder Analysis

Slide 31

Communication Plan Example

Key Message	Stakeholder	Communication	Channel	When	Responsibility	Status
The new methodology has an evidence base that supports it as superior teaching practice	Head of School	Paper that provides the evidence based research that supports the new initiative	Email followed by face to face	End of June	Mary and John	Completed
		Progress reports	Email	Monthly	Mary and John	Not yet commenced
	Academic Staff	Presentation to staff demonstrating the new technology and progress	Staff meeting	End of July then monthly	Mary	On-track
	ITS	Discussion on the technical requirements for the new innovation	Meeting	End of July	John	On-track
		Implementation steering committee progress reports	Meeting papers	Fortnightly	Mary and John	On-track
All academic staff will receive professional development in the new methodology	Academic staff	Training plan with dates and times	Email	End of August	John	On-track
	TEDI	Training requirements	Meeting	End of July	Mary	On-track

Communication management

Slide 32

Preparing for crisis communication

- Stakeholder communications focus on consulting internal and external stakeholders on the conduct of the BCM process and planning procedures
- Crisis communication focuses on the **provision and receipt of information relating to the management of an incident**
- ***If an event happens, we need to*** communicate the nature of the event, the emergency response, the organisations continuity activity, the range of restoration and recovery activity
- It needs to be a strategic plan/s
  - Identifying the objective, e.g. to keep staff informed, inform key customers, communicate with public
  - Who is involved, who has responsibility, who is communicated with

Some possible considerations

Slide 33

- Who leads the crisis communications? Who communicates publicly? .. E.g. to media Who leads communications internally?
- Can you Identify all personnel who should be notified when a DRP / crisis communications plan is activated. Are their personnel with specific responsibilities within the plan?
- Are communications channels established? IT-based, such as e-mail or instant messenger. Mobile phones or two way radio? Specific meeting times in a central location such as a "war room" instead of using electronic communications?
- Who are the users to be notified if the DRP Crisis affects them? For example, critical business operations may not include some routine functions or areas
- Should customers be notified if a disruption affects them?

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

33

Communication management

Slide 34

Preparing for crisis communication

- Do we have a documented, proactive crisis communications plan?
- Have we identified and trained all the internal resources required to execute the communications plan?
- Do we have contacts at specialist crisis communications firms if we need their services?
- In the case of a cybersecurity event involving personally identifiable information (PII), do we have a system in place to quickly determine who should be notified, and how?
- i.e. crisis communication is part of the incident response / or disaster recovery plan
- Is there a crisis response team in place? Assessment for communication needs to be part of the process
- Have we templated a time line for response?

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

34

Communication management

Slide 35

Preparing for crisis communication

Table 17a
The IRACI tool

Communication action	Description
Intervention	Who has sufficient authority to intervene to halt a communication or would need to become involved if issues arise following the communication (eg adverse reaction to the communication).
Responsibility	Who has the responsibility for undertaking the communications.
Accountability	Who has the accountability for the communications, including approval of content and authorisation for release.
Consult	Who needs to be consulted as part of the communications process.
Inform	Who needs to be provided with the final communication on its release.

Table 17b
Example of the use of the IRACI tool

Intervention	Responsibility	Accountability	Consult	Inform
Issue 1: Stakeholder communication regarding loss of service				
Chairman of the Board	Public relations officer	Assistant manager stakeholder communications	General managers of operational divisions	High priority stakeholder groups
Issue 2: Supplier communication regarding establishment of recovery site				
General manager corporate services	Purchasing officer	Contracts manager	Building services manager Managers of critical business functions	Suppliers Affected staff

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

35

Thank you

Assignment questions to F2F class please, or in Canvas discussion forum

SWINBURNE UNIVERSITY OF TECHNOLOGY

Swinburne think forward

36