



Welcome to INF30020 Lecture 8

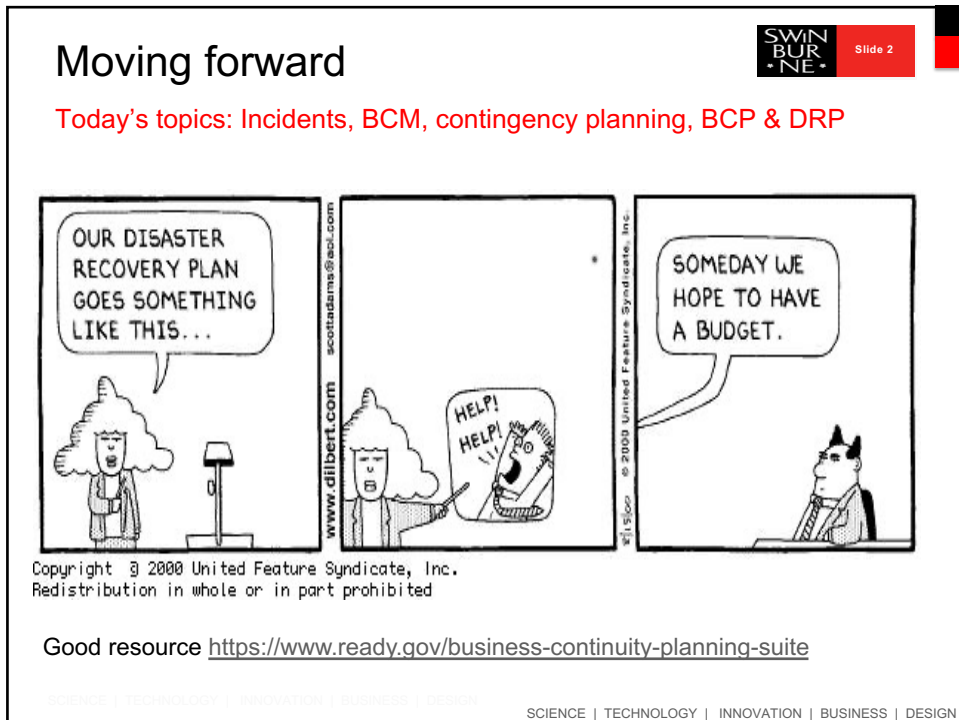
Key topics in Business Continuity Management and contingency planning

**Swinburne**  
▶ think forward

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

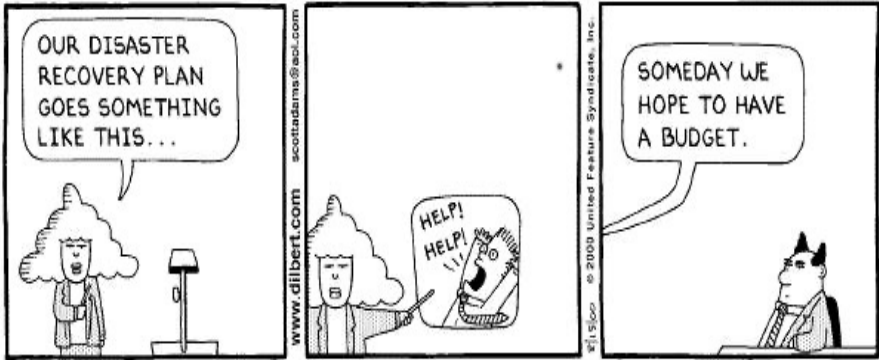
CRICOS Provider: 00111D | T.O.D.: 3059

1



## Moving forward

Today's topics: Incidents, BCM, contingency planning, BCP & DRP



Copyright © 2000 United Feature Syndicate, Inc.  
Redistribution in whole or in part prohibited

Good resource <https://www.ready.gov/business-continuity-planning-suite>

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

2

## Summary, schedule and assessment

SWIN  
BUR  
NE

Slide 3

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

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

3

## This week's learning plan

SWIN  
BUR  
NE

Slide 4

### Gain an understanding of

- The role of
  - Business continuity management
  - Contingency planning
  - Contingency plans
  - Business continuity planning (BCP)
 in information security and risk management
- Key concepts in BCM planning including
  - Incident response (more focus in week 9)
  - disaster recovery
- Information Auditors role in BCM & DRP
- Responses: Backup and site options (also see extended slides)

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

4

## Week 8's learning plan



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

Both week 8 and week 9 (& 10) are critical for CLA#3 and your group assignment

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

5

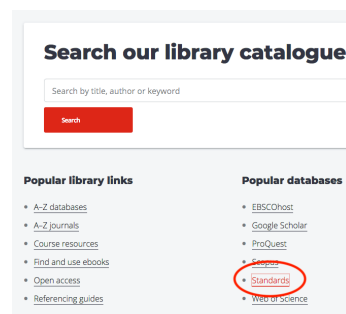
## Reading for this week's topic

### Unit texts:

- **Whitman, Michael E. and 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 Tech Street Database)**
- **Whitman Chapters 7, 10**
- **Gibson Chapters 11- 15**



SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

6

## Business continuity management



### BCM Standards and guidelines (ISO 22301: 2019)

- HB292-2006 – (A Practitioners Guide to Business Continuity Management , Swinburne Library Standards 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

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

7

## Incidents, disasters and response



### Risk management – response versus recovery

The key to business continuity management is understanding information security and risk management



**Understanding the likelihood of an unwanted event occurring and managing its impact is the first step to ensuring business continuity**

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

8

## Incidents, disasters and response

SWINBURNE  
Slide 9

### Incident

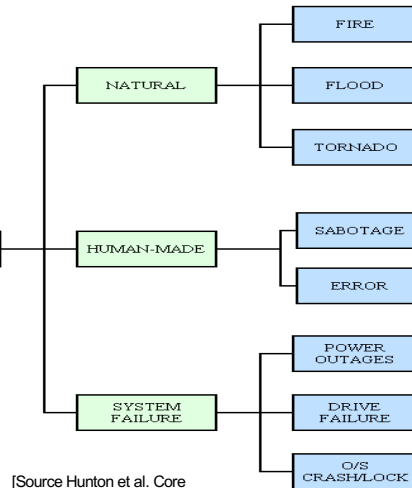
An incident is any business disrupting event including any emergency (a crisis or disaster), its our broadest concept

In terms of information security it will include any information systems disruption: i.e. An unplanned event that causes information systems to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).



Incidents

Figure 2.6: Types of Disasters



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

BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

9

## Incidents, disasters and response

SWINBURNE  
Slide 10

### Human made

As Data Breach Woes Continue, Target's CEO Resigns

Ryanair remains tight-lipped over £3.3m hacker theft

Higher Ed Ransomware Attack: University Pays \$457K Despite Having Backups



Optus faces a customer exodus, calls for compensation amid anger over leaked data

Current and former Optus customers are demanding help in safeguarding their personal information, with an expert saying the level of risk varies from person to person.



technology

Aussies 1 continue

is servers npts

- ① Human Error
- ② Viruses & Malware
- ③ Hard Drive Damage
- ④ Power Outages
- ⑤ Computer Theft
- ⑥ Liquid Damage
- ⑦ Disasters
- ⑧ Software Corruption
- ⑨ Hard Drive Formatting
- ⑩ Hackers and Insiders

SCIENCE | TECHNOLOGY

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

10

# Incidents, disasters and response

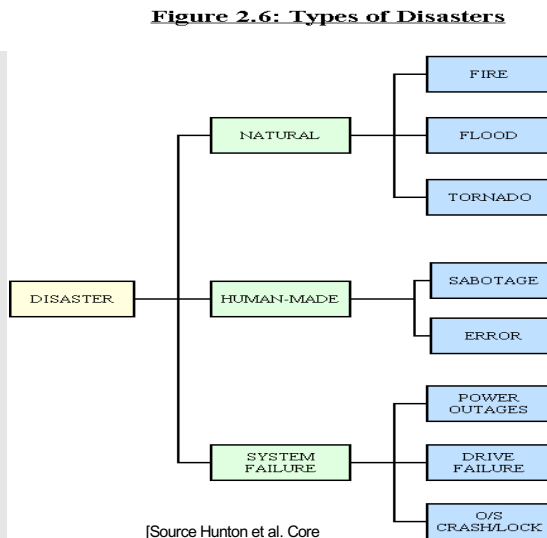
SWINBURNE  
Slide 11

## Disaster

A sudden, unplanned *calamitous event causing great damage or loss*.

1. Any event that creates an inability on the organisation's part to provide critical business functions for a period of time
2. The period when the organisation's management decides to divert from normal production responses and exercises its disaster recovery plan. Typically signifies the beginning of a move from a primary to an alternate location.

**Disruption, Damage, Denial, Disaster (4Ds Kevin Fitzgerald – InfoSec Consultancy Melbourne)**



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

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

11

# Incidents, disasters and response

SWINBURNE  
Slide 12

## Natural disaster

**Superstorm hits Australia's east coast with 4000 lightning strikes in one hour in Brisbane**

**Natural Disaster Downtime 1**

Study of 79 Internet and found that storms -- longer outages than c

When it comes to down

That's one disaster reco

Annual Incident Reports

Network and information

The report is based on 7 communication networks serious incidents -- which report -- on a sliding scale affect 15% or more of all users affect 1% or more of all users

All told, 18 European countries reported having a total of 79 "significant incidents" to ENISA, while nine other countries said the incidents.

Twitter users should reassign access to third-party apps: Hacker Leaks 15,000 Twitter Access Credentials. [More.]

Downtime is a major concern for businesses and governments. When systems are down, employee productivity plummets, subscribers can't be billed and emergency services are affected. The report assessed four different types of service outages: telephone and fixed Internet, and mobile telephony and mobile Internet.

The Australian.com.au

62,000 without internet

By David Kirkpatrick  
Updated March 2 2022 - 12:25pm, first published 1:00pm



Kleen St, Lismore on Wednesday. Photo: Cathy Adams

**Internet banking outages amid Lismore floods highlight need for cash**

By Harrison Ashbury on March 09, 2022  
Fact Checked

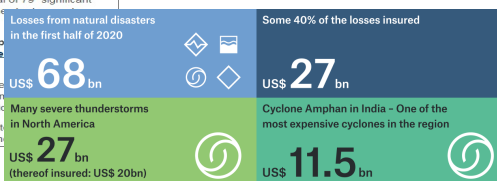


Signal outages caused by flooding in Lismore have rendered ATMs and mobile banking in the area largely unusable, leaving many residents with no access to funds.

darkreading.com

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

© Munich Re NatCatSERVICE



SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

12



## Incidents, disasters and response

SWIN  
BUR  
NE

Slide 13

### Information Systems & IT failure (natural disaster & human error)

#### Telstra sorry for north Qld outage

Posted 29 Jan 2013, 10:21am

Telstra has apologised for a major outage that cut communications in the northern half of Queensland.

MAP: QLD

Since the weekend, landlines, mobile phones and internet access after flooding damaged cables near Bundaberg and Kingaroy.

{\* CLOUD \*}

#### AWS celebrates Labor Day weekend by roasting customer data in US-East-1 BBQ

Postmortem report: Power outage knackered instances, volumes for unlucky punters

Customers turned to social media to vent their anger, with many posting they were fed up with the outages.

Telstra said it experienced issues, like "many of its global peers".

"There will always be issues that arise in such a large and complex technology environment," a spokesman said.

"We are committed to redoubling our efforts on resilience in the network, and part of that is conducting a major review in relation to the outages from last week and February."

hundreds and about 100 businesses in several towns across the Kimberley and Pilbara.

Telstra has apologised for the inconvenience.

A power outage fried hardware within one of Amazon Web Services' data centers during America's Labor Day weekend, causing some customer

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

13

## Incidents, disasters and response

SWIN  
BUR  
NE

Slide 14

### What are the drivers for response and recovery?

- Absolute dependence on IT and stored data
- Pressure from clients / market / competitors
- Regulatory pressure (*banking and finance – e.g. APRA requirements*)
- Federal & state government guidelines (*public sector*)
- Corporate governance
- Public Image
- Uncertain global climate with recent significant increase in the impact of both natural disaster and cyber-crime
- **Business continuity and survival**

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

14

## Incidents, disasters and response

SWINBURNE

Slide 15

*Incidents are far reaching....*

- E-commerce down
- Applications down
- Lost billings records
- Lost business information

- Used against you
- Lost business
- Lost market share
- Higher expenses
- Opportunity Costs

- Customer perception
- Investor uncertainty
- Lender uncertainty
- Hiring slowdown
- Employee turnover
- Impact to brand and image

**Lost revenue**

**Business interruption**

**Competitiveness**

**Litigation**

**Company reputation**

- End-users cannot do their jobs
- IT operations disrupted
- Customers cannot access data
- Suppliers cannot complete service
- Higher phone volume
- Lost orders
- Customer care calls disconnected

- Investor filings
- Supplier misunderstandings
- Customer contracts unmet
- Service levels unmet

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

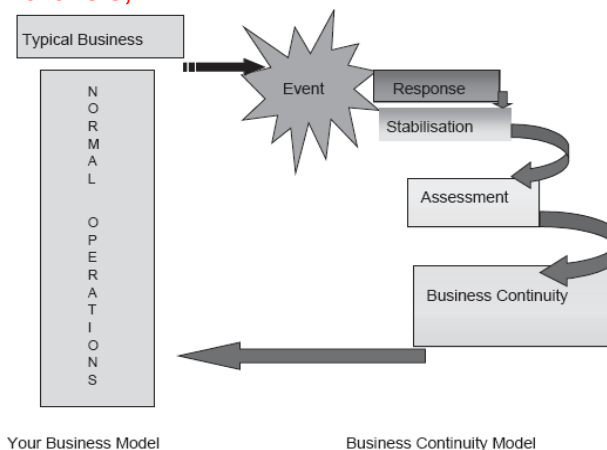
15

## Incidents, disasters and response

SWINBURNE

Slide 16

*Incident Response not recovery - Maintaining business through a crisis,*



Castillo, 2004

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

16



## Business continuity management



### BCM and Contingency planning (...the differences are...?)

- Business continuity management is the development, implementation and maintenance of **policies, frameworks and programs** to assist an entity manage disruption to its business (ANAO, Best practice guide)
- **Management policy and procedures designed to maintain or restore business operations**, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters. (US NIST 800:34)
- Largely one in the same. In this unit we take primarily an holistic BCM approach, seeing **contingency planning** as focussing on the definition of subordinate plans implemented to manage contingencies (e.g. the occurrence of disruptive events; applying crisis communication strategies etc.), - **COOP, DRP, Incident response plans and crisis communications plans are types of contingency plans**



SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

17

## Business continuity management



### BCM Holistic view .... think COSO ERM

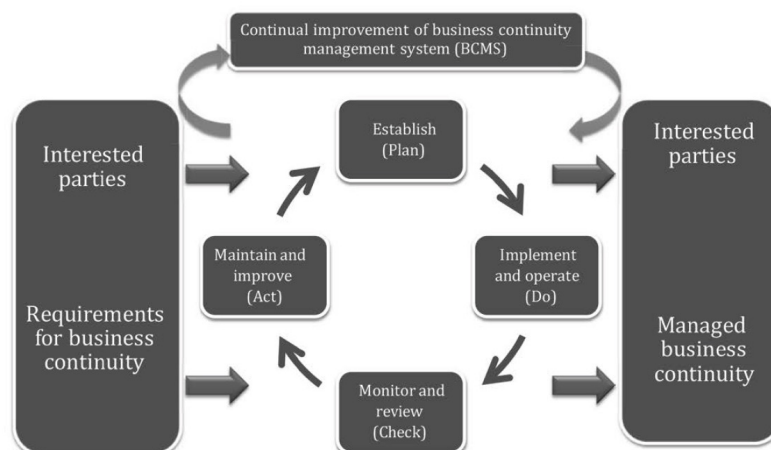


Figure 1 — PDCA model applied to BCMS processes

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

18

## Business continuity management



### BCM Defined

- Business continuity management is the development, implementation and maintenance of policies, frameworks and programs to assist an entity manage a business disruption, **as well as building entity resilience**. It is the capability that assists in preventing, preparing for, responding to, managing and recovering from the impacts of a disruptive event. (ANAO, Best practice guide 2009. pg2)

BCM involves:

- ✓ being clear on the organization's key products and services and activities that deliver them (*information assets*);
- a) knowing the priorities for resuming activities and the resources required;
- b) having a clear understanding of the threats to activities, including their dependencies;
- c) knowing the impacts of not resuming activities;
- d) having tried and trusted arrangements in place to resume activities following a disruptive incident; and
- e) making sure that these arrangements are routinely reviewed and updated so that they will be effective in all circumstances.

**BCM understood:** Create realistic, uncomplicated and practical response and recovery processes to ensure survivability

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

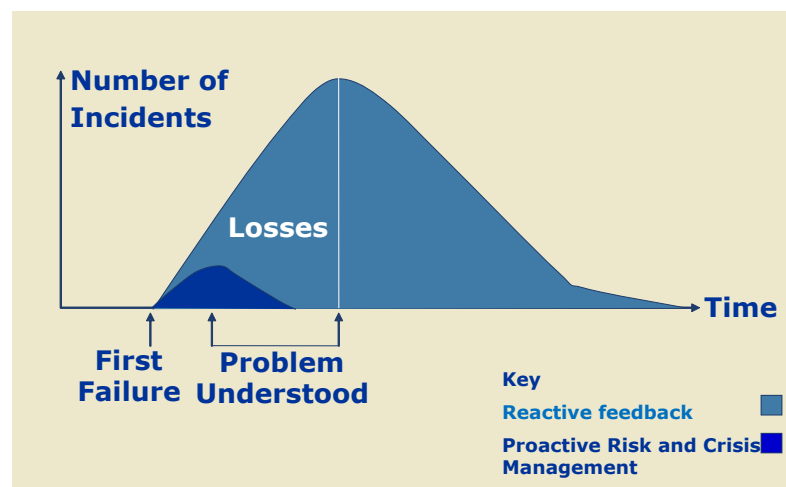
SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

19

## Business continuity management



### Benefits of BCM and planning for contingencies



SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

20

## Business continuity management



### Business continuity planning (BCP) and disaster recovery (DRP)

- Business continuity plan: those activities intended to ensure the ongoing running of an organisation during the period of disruption of normal operation
- Incident response plan: focuses on immediate information systems security responses to incidents affecting systems and networks
- Disaster recovery plan: refers to those activities required to minimize the the disruption on the organization and recover from a loss, either short or long term, especially in terms of information processing facilities
- Preventative controls are never 100% effective, so controls must be in place to mitigate the effects once a disruption has occurred
- Control planning must be based on the assumption that any computer system is subject to multiple types of failures. Procedures must exist and must be tested for recovery from failures, losses of equipment, applications and data

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

21

## Business continuity management



### Business continuity planning (BCP)

- **Is the process of creating and validating and implementing a business (based) plan for maintaining continuous operations before, during, and after disasters and disruptive events.**
- Involves developing arrangements and procedures that enable an organisation to respond to an event in such a manner that critical business functions continue when normal operations are disrupted
- It allows us to consider issues like Max allowable downtime, Seeks to prevent interruption of mission-critical services; and to reestablish full functioning as swiftly and smoothly as possible after interruption.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

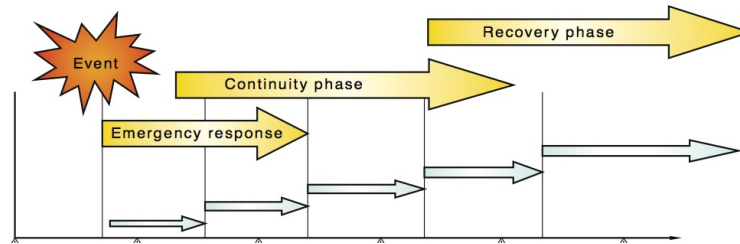
22

## Business continuity management

SWINBURNE  
Slide 23

### Planning for business continuity and disaster recovery

The identification and prioritization of a response and recovery process



HB292-2006 – A Practitioners Guide to Business Continuity Management

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

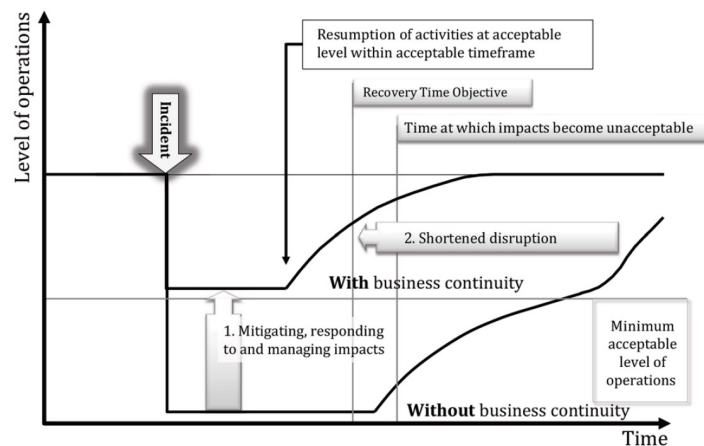
23

## Business continuity management

SWINBURNE  
Slide 24

### The BCP proposition: optimise the recovery time

Mitigating impacts through effective business continuity – sudden disruption



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

Figure 2 — Illustration of business continuity being effective for sudden disruption

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

24

## Business continuity management



Business continuity planning (BCP), *a plan for response*

- Continuation of critical services regardless of the event.
- **The event is not the most relevant aspect– the focus is on**
  - **Identification of critical business functions (BIA)**
  - Identification of risks to those functions
  - Risk prioritisation- impact vs. probability
  - Risk avoidance or mitigation recommendations
  - **Response and recovery**

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

25

## Business continuity management



Planning for business continuity and/or disaster recovery

- **Strategic context** for business continuity
  - Role and purpose of BCM who the intended audience is
- **Risk assessment is the foundation:** identifying threats and assessing the impact and likelihood
- **Identifying the consequences of disruption:** disruption scenarios (i.e. multiple disruptions resulting in a loss of access to the building) and from there, business impact analysis
  - E.g. loss of revenues; delays in invoicing & payment; lost interest; lost sales; lost future business; incurred costs; extra staffing; loss of discounts; inefficiencies
  - Degrees of priority can be associated with different information process, e.g. a business loss rating, service levels required, assessment of maximum down time that is tolerable
- **Identification and prioritization of a response** and recovery process
- **Commonly omitted issues include**
  - Teams, training and rehearsals
  - inter-relationships between systems, accommodation, people, stationery supplies, office equipment, control procedures

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

26

## Business continuity management



### Disaster recovery plan, .... a plan for recovery

A Disaster Recovery Plan (DRP) is a comprehensive statement of all actions to be taken **before, during, and after a disaster**, along with documented, tested procedures that will ensure the continuity of operations. Organisations, and nations states plan and test their disaster response

Two aspects:

- Disaster Prevention (DP):  
The process of minimizing the risk of a disaster occurring. Pre-disaster steps taken.
- Disaster Recovery (DR):  
The process of minimizing business operation downtime in the event of a disaster. Post-disaster steps taken

It includes specifying:

1. Safe Location
2. Resources Available
3. Systematic Process for Recovery
4. Reliable Plan (i.e., tested)

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

27

## Steps for Implementing a BCP

1. Create BCM guidelines & scope statements
2. Identify & prioritise information assets to be safeguarded
3. Conduct business impact analysis (BIA)
4. Identify countermeasures and controls
5. **Develop simple/general contingency plan**, e.g. incident response &/or disaster recovery plans (DRPs)
6. Implement training
7. Test and exercise plans
8. Maintain and update plans

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

28

## Business continuity management



### For recovery purposes, the important steps....

- The minimum configuration required with steps for recovery put in writing
- BCM governance established with chief officer and committee
- Critical applications, information processes and data identified
- Whether continuity arrangements with vendors exist (also insurance arrangements .... *i.e. sharing risk*)
- Hot and cold site solutions determined
- Backup procedures that have been agreed (with offsite solutions in place)
  - Security arrangements that have been agreed to
  - Compatibility of equipment, hardware, software
- Manual procedures in place and tested
- Testing is carried out regularly and successfully
- **Communications plan in place, emergency numbers, staff management**

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

29

## Business continuity management



### Auditing (*and testing!*) the BCM plan (including BCP, DRP)

- Systems auditing ensures management has **implemented controls** to a reasonable level of assurance
- Verify the **adequacy of the plan**: determine that the plan as formulated can give the organization the capability of short term recovery and return to full operation in the long term (reasonable time frame and reasonable costs)
- Involves assessment of the organizations **criteria for development of the plan**
- Determine the effectiveness of the plan's implementation: establish **management records of testing the plan across a variety of categories of disaster** (ranging from minimal disruption to full-scale unavailability); determine that the test were effective
- Determine mechanisms for the management of the plan (including how it is kept up to date); **ensure plan is maintained** and reflects current business state
- **Ensure responsibility** for plan maintenance; ensure management are kept informed; ensure master copy of plan is secure; ensure distributed copies are kept up-to-date

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

30



## Business continuity management



### Auditing (*and testing!*) the BCM plan (including BCP, DRP)

- Maintaining protection for:
    - Physical access
    - Fire protection
    - Water protection
    - Power supply and reticulation
    - Air conditioning supply and reticulation
    - Data and Voice Communication
    - Other infrastructure/s e.g. BYOD...ICT...Cloud...Big Data...
- ...All areas must consider - prevention; detection; alarm and response systems; redundancy of equipment; plus testing and reviewing of maintenance records

**Backup and restoration and resumption are carefully planned for**

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

31

## Business continuity management



### Business resumption plan (BRP), the steps for coming back

- The process of planning for and/or implementing the restarting of defined business operations following a disaster, usually beginning with the most critical or time-sensitive functions and continuing along a planned sequence to address all identified areas
- The BRP addresses the restoration of business processes after an emergency, but unlike the BCP, lacks procedures to ensure continuity of critical processes throughout an emergency or disruption.
- Development of the BRP should be coordinated with the disaster recovery plan and BCP.
- The BRP is usually 1 part DRP and 1 part BCP because DRP manages the efforts to resume normal operations, and the BCP contains steps for resuming critical business operations

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

32

## Continuity of operations



### Lessons Learned from 9/11

*“In the aftermath of the attack on the World Trade Center virtually all of Pace's means of communication were inoperable; **cell phones, regular telephones, and Internet service were disabled.** Fortunately, the school's email network was functioning, and administrators were able to communicate with each other. Yet, no plan addressed how administrators would have communicated with one another had the university's intranet not been functioning.”*

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

33

## Hurricane Katrina

<https://www.youtube.com/watch?v=2LA31bhsvNo>



### Experience of Hurricane Katrina (CEOs at 2005)

- **HOWARD SCHULTZ**, *chairman, Starbucks*, ‘We told the vendor they needed to create a way for us to do text messaging. The voice part collapses too easily’
- **J.W. MARRIOTT JR.**, *CEO, Marriott International*, ‘The most important thing in dealing with any crisis is communication, so we moved our e-mail system out of New Orleans’
- **JIM SKINNER**, *CEO, McDonald's*, ‘We needed a central command center, and we handled about 3,800 calls’
- **BOB NARDELLI**, *CEO, Home Depot*, ‘I couldn't get gasoline’
- **PAUL PRESSLER**, *CEO, Gap*, ‘employees live paycheck to paycheck. One thing we're going to do is encourage more employees to set up direct deposit’
- **DUANE ACKERMAN**, *CEO, BellSouth*, ‘What we learned from that was we needed to move our telephone switches to higher elevations’

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

34

## Business continuity management



### Continuity of operations plan

- **The process to restore an organization's (usually a headquarters element) essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations**
- Because a COOP addresses headquarters-level issues, it is developed and executed independently from the BCP
- Standard elements of a COOP
  - Delegation of authority statements,
  - Orders of succession, and
  - Vital records and databases
- minor disruptions that do not require relocation to an alternate site are typically not addressed
- Because the COOP emphasizes the recovery of an organization's operational capability at an alternate site the plan does not necessarily include IT operations.
- COOP may include the BCP, BRP, and disaster recovery plan as appendices.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

35

## Crisis communication



### Experience of Hurricane Katrina (CEOs at 2005)

An important component of any incident preparedness program is the crisis communications plan. A business must be able to respond promptly, accurately and confidently during an emergency in the hours and days that follow. Many different audiences must be reached with information specific to their interests and needs. The image of the business can be positively or negatively impacted by public perceptions of the handling of the incident.

<https://www.ready.gov/business/implementation/crisis>

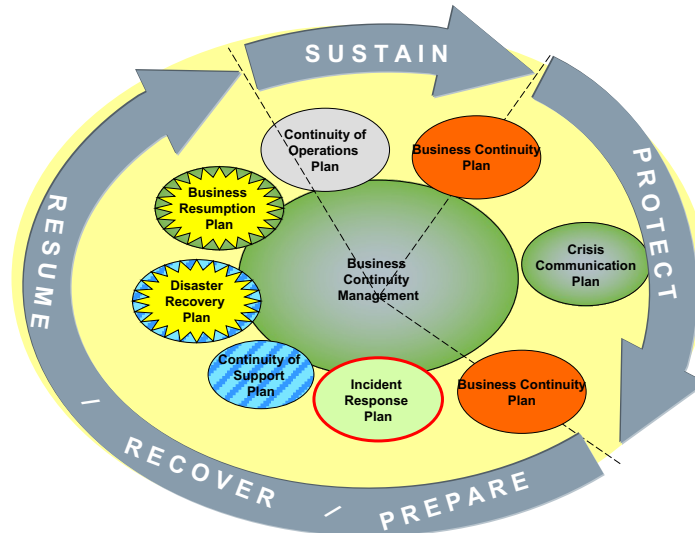
SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

36

## Business continuity management

SWINBURNE

Slide 37



Based on SP 800-34

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

37

Thank you & your questions

SWINBURNE

SWINBURNE  
UNIVERSITY OF  
TECHNOLOGY

Terms to follow up on

1. Incidents, disasters and response
2. Business continuity management
3. Contingency planning
4. Business Continuity plan and Disaster recovery plan
5. Responses: Site management and backup

**Swinburne**  
▶ think forward

38