INFO6027
Information Security Planning

Lesson 6

FANSHAWE

Housekeeping

- “**Mid Term” grades** will be submitted later today. You will receive an **S** or **U**.
  - Reminder about peer tutors

- **Test #1**
  - Overall very well done.
  - What were your thoughts on the test (ex,. time, process, difficulty, etc.)? Any strategies to share?

Lesson 6: Contingency Planning

This Lesson will cover:

1. Contingency Planning (CP)
2. DRP
3. BCP Policy
4. The 5 Phases of BCP

What is in the news today, yesterday, last week, last month, last year? ☺

- **North Korea Hacked Him. So He Took Down Its Internet** **https://www.wired.com/story/north-korea-hacker-internet-outage/**
- **Out-of-Control Cybercrime Will Cause More Real-World Harm**
- Ransomware and online attacks can lead to deadly real-world consequences. Governments need to raise their game in response. https://www.wired.com/story/cyber-criminals-physical-harm/
- https://krebsonsecurity.com/category/data-breaches/
- Choosing a DRP: https://olmec.com/choosing-right-disaster-recovery-plan/ also, https://ctscomplete.com/blog/7-reasons-you-need-a-disaster-recovery-plan/

DRP in the News…

Disaster recovery now a priority

By GERHARD FOURIE, district channel manager for Commvault South Africa

Published 2 days ago on February 16, 2021

Research From iland Shows a Lack of Focus on Disaster Recovery

Posted on February 12, 2021 by Tess Hanna in Backup and Recovery Solutions News

Broward County Public Schools Projected to Save an Estimated $2.3 Million in Disaster Recovery After Deploying Veeam for Data Backup and Protection

Broward County Public Schools replaces Commvault with Veeam to mitigate the risks associated with data loss while also supporting compliance with FERPA, HIPAA and Florida's Sunshine Law

Why 2020 Was the Year of Disaster Recovery

These three trends remind us of the value of our data.

By Patrick Doherty

January 19, 2021

Disaster Recovery Planning Includes Ensuring That Data Can Be Recovered

Written by Carbonite Guest Blogger February 16, 2021

Here's how to ensure that your disaster recovery solution will work when it matters.

Q & A time!

1. What is Business Continuity Management (BCM) and is it different from Business Continuity Planning (BCP)?
2. *Describe* (don't just state) the 5 phases of business continuity planning?
3. What is DRP? (define *both* the acronym and the term)
4. What is a "contingency"?
5. What is the relationship between BIA and contingency planning?

Contingency Planning (CP)

FANSHAWE

Sample Scenario: What's the problem?

- Some companies outsource their DNS services, especially if they host web servers outside of the company data center.

The good:

- You have *transferred* the risk of a DNS failure (which could be a disaster) or a DNS-based cyber attack ☺

The bad:

- The same failures can happen to the service provider so…
- The risk is still there, and now
- It's out of your control
- Back-up systems are difficult to peer together.

The point of this exercise?

- Regardless of the strategy, we must still **accept** some risk and have a **Contingency Plan** for **Incident Management** and **Disaster Recovery**.

Some context before we begin…

- Please read the following article…

DATA CENTERS

The major lesson IT can learn from Netflix's high availability testing methodology

High availability events are more likely to be triggered then disaster recovery events, but often aren't tested for as much. Here's what tech leaders can take away from Netflix's approach to the problem.

By Keith Townsend | June 6, 2016, 5:52 AM PST

What is Contingency Planning (CP)?

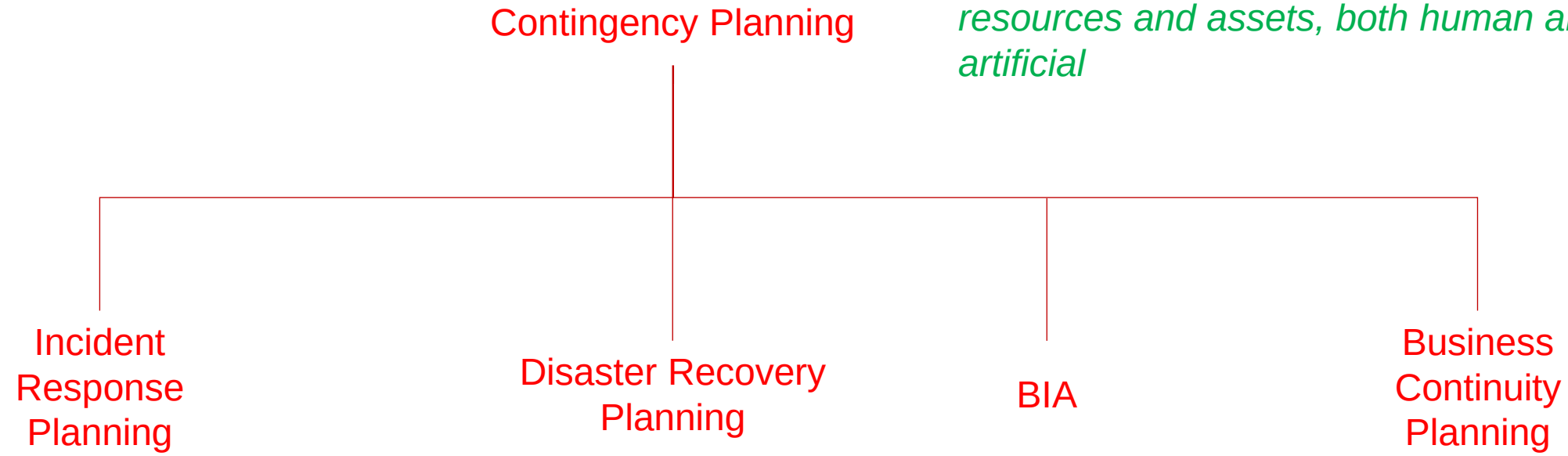
- Comprised of IRP, DRP, and BCP
- A long-term plan to ensure the *continuity of business operations*.
- The process of creating **systems of prevention and recovery** to deal with potential threats to a company
- Any event that could negatively impact operations is included in the plans, such as supply chain interruption, loss of or damage to critical infrastructure (major machinery or computing /network resource).
- As such, **risk management is part of CP**
- Covered by two separate domains of CISSP CBK
  1. Security and Risk Management
  2. Security Operations

How Does CP Fit In With What We've Already Learned?

Contingency:

- *"a provision for an unforeseen event or circumstance."*

CP is the process by which the IT and InfoSec communities position their organizations to prepare for , detect, react to, and recover from events that threaten the security of information resources and assets, both human and artificial



The CP domains address:

- Continuation of critical business processes when a **disaster** destroys data processing capabilities
  - Businesses define "**disaster**" differently. Why?
- Preparation, testing and maintenance of "specific actions to maintain (or recover) normal processing" (aka the BCP)

Disaster Recovery Plans

FANSHAWE

DISASTER RECOVERY PLANS

- What would be disastrous to your business?

Disasters can be both Natural and Man-made

- Natural disasters include:
  - Fire, flood, hurricane, tornado, earthquake, volcanoes, lightning strike, landslide/mudslide, typhoon, tsunami,
- Man-made disasters include:
  - Plane crashes,
  - vandalism,
  - terrorism,
  - riots,
  - sabotage,
  - loss of personnel, etc.
- Disaster can be defined as “Anything that diminishes or destroys normal data processing capabilities”. Disasters are defined in terms of the business.

Disaster Recovery Planning (DRP)

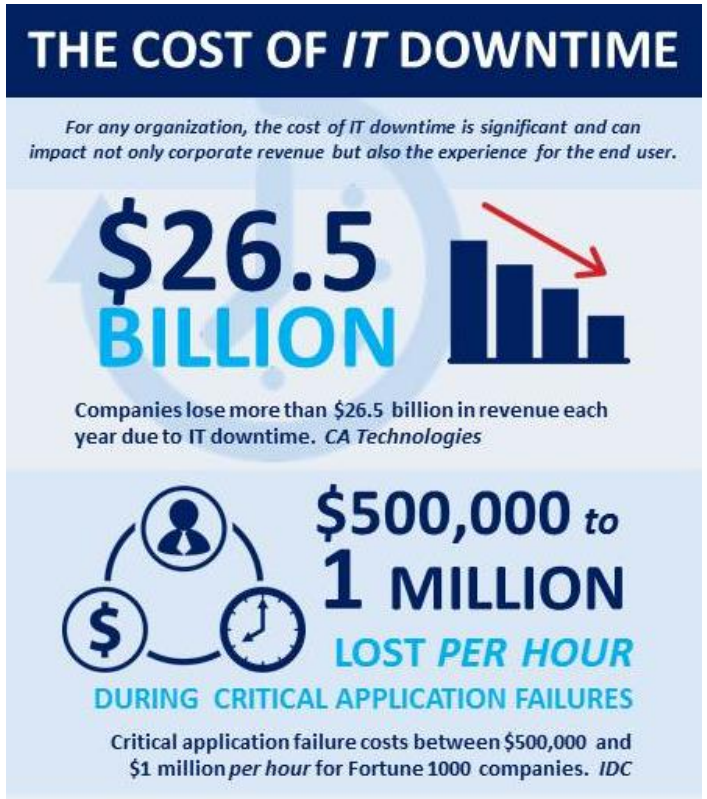
- Entails the *preparation for* and *recovery from* a disaster, whether natural of man-made.
- **DRP is created by the CP Team**
- Invoked when either:
  1. Organization is unable to contain or control the impact of an incident
  2. The level of damage or destruction from an incident is so severe that you cannot quickly recover from it
- Could basic Incident Response ever be escalated to Disaster Recovery?
  - YES! ex. Malicious code detected is an incident, but what happens if that code cripples the organization?

Disasters are defined in terms of the Business

- If it harms critical business processes, it may be a disaster
- Probability of occurrence / severity of occurrence
- Disasters are often a **time-based definition** that is best represented as *Cost of Downtime* in $$ per hour.
  - Time really is money! More downtime = More money lost

- "A business disaster is that point in time after the "cause" when you **cannot provide your customers and users with the minimum** level of services they need and expect"
  - Eg. Backhoe cuts the fiber line into small software business, or their ISP goes out of business…

According to Gartner, the average cost of IT downtime is $5,600 per minute. Because there are so many differences in how businesses operate, downtime, at the low end, can be as much as $140,000 per hour, $300,000 per hour on average, and as much as $540,000 per hour at the higher end.



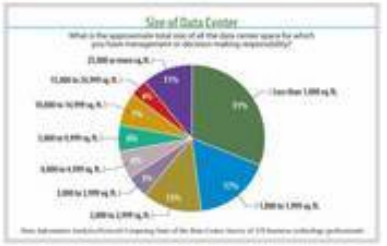
https://martellotech.com/blog/the-cost-of-it-downtime/

IT Downtime Costs $26.5 Billion In Lost Revenue

Still, 56% of enterprises in North America and 30% in Europe don't have a good disaster recovery plan, says a CA Technologies survey of 200 companies.

It can be difficult to measure the cost of IT failures. For example, how do you measure outages such as those that recently hit Amazon Web Services or Sony's Playstation Network?

CA Technologies is the latest to attempt to calculate IT downtime, with a survey of 200 companies across North America and Europe intended to calculate the losses incurred from an IT outage. What it found was more than $26.5 billion in revenue is lost each year from IT downtime, which translates to roughly $150,000 is lost annually for each business.



Analytics Slideshow: 2010 Data Center Operational Trends Report

(click for larger image and for full slideshow)

The survey also found that IT outages are frequent and lengthy, and they cause substantial damage to a company's' reputations, staff morale, and customer loyalty. And they can rattle the confidence in new technologies such as cloud computing.

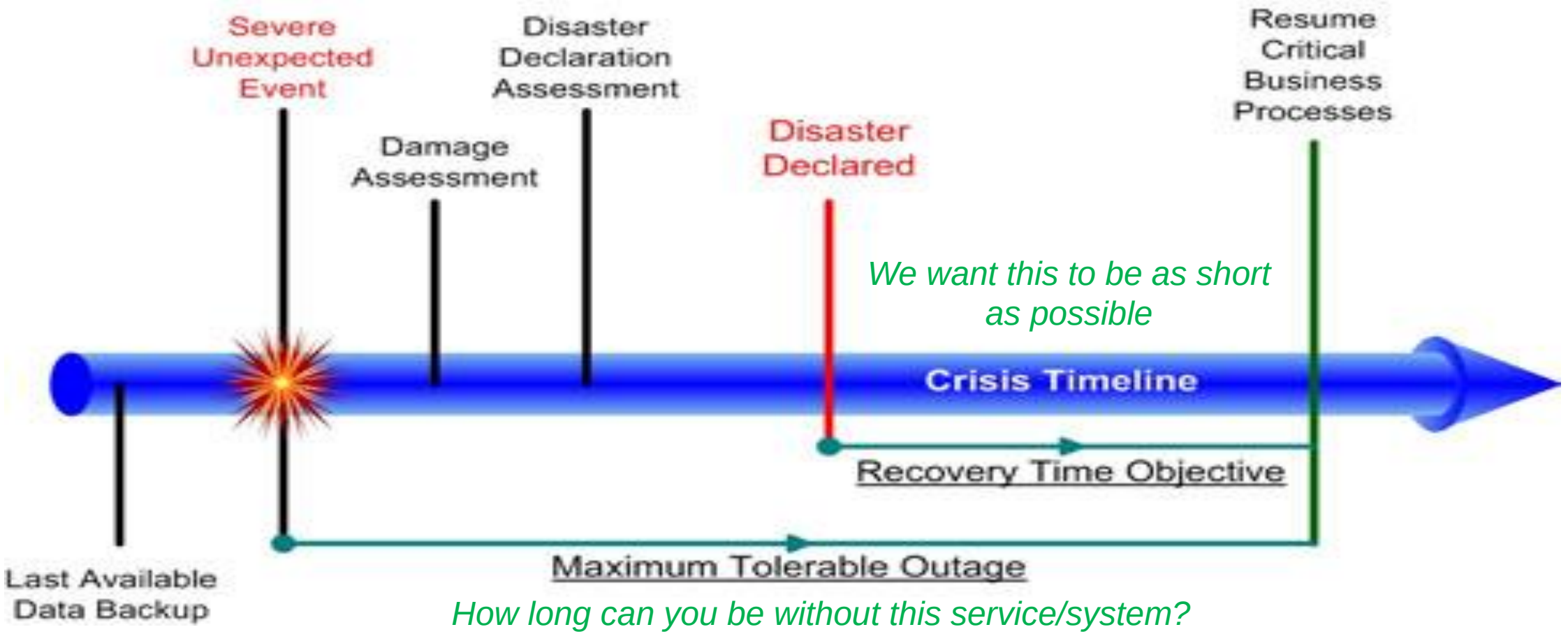
On average, the businesses surveyed said they suffered 14 hours of IT downtime per year. Half of those said IT outages damage their reputation and 18% described the impact on their reputation as "very damaging."

https://www.informationweek.com/it-downtime-costs-$265-billion-in-lost-revenue/d/d-id/1097919

FANSHAWE

Types of Disasters

Natural	Earthquakes, floods, storms (i.e., thunder, hail, lightning, electrical, snow, winter ice), tornadoes, hurricanes, volcanic eruptions, natural fires
System/ technical	Hardware/software outages, programming/system errors
Supply Systems	Communication outages, power distribution (i.e., blackouts), burst pipes, manufacturing interruptions, delivery interruptions, etc.
Man-made	Bombings, explosions, disgruntled employees, fires, purposeful destruction, aircraft crashes, hazardous/toxic spills, chemical contamination, malicious code
Political Events	Terrorist attacks, espionage, riots or civil disturbances, strikes



How long can you be without this service/system?

How to Categorize **Potential Loss from a Disaster**

- Operating Costs
- Revenue Loss.
- Compromised Customer Service.
- Embarrassment or **Loss of Confidence** Impact
- Advantage to Competition

https://bit.ly/3jGlC1g

- All categories can be **quantified by CoD**
- There are extra costs involved in creating and utilize DR and BC Plans,
  - **Do the Benefits of Continuity Planning offset these costs?**

7 Steps of DRP (can be used for IR and BC as well)

1. Develop the DR planning policy statement
2. Review the BIA
3. Identify Preventative Controls
   - Controls are measures taken place to reduce the impact of disruptions
4. Develop recovery strategies
5. Develop the DRP document (detailed guidelines and procedures for restoring a damaged system)
6. Plan testing, training, and exercises
7. Maintain the plan! (this is a living document – update it regularly!)

Disaster Recovery Planning (DRP)

- What comes before Disaster ***Recovery***? (hint: "disaster _____")
  - **Which is cheaper – Avoidance or Recovery?**
- How do we preserve **critical** business functions in the face of a disaster?
- If you cannot avoid 100% then you must have **recovery plans** (ex. IR and DR)
- BCP vs DR: Business Continuity Planning is often managed by the CEO/Board, while Disaster Recovery is usually handled by the IT community of interest
- Both plans can (and usually do) run at the same time – especially if the disaster is major or long term.
  - Often combined into one plan, called a Business Resumption Plan

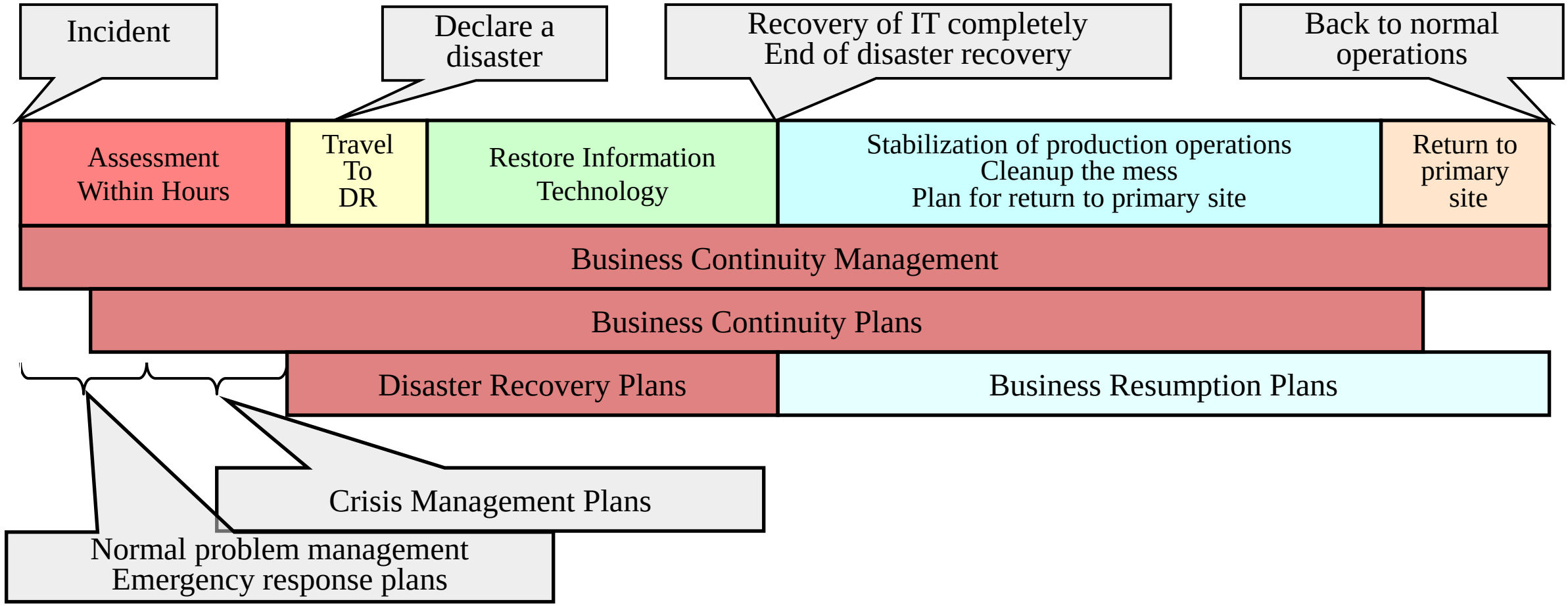
Some Disaster Statistics (Rock, 2020)

According to Research

- 1 in 5 companies don't have a disaster recovery plan
- 54% of companies have experienced prolonged downtime
- 40-60% of small businesses never reopen after a disaster
- 90% fail if they don't reopen quick enough (they exceed their MTD)
- 60% of backups are incomplete
- 93% of companies went bankrupt after prolonged data loss
- 37% of SMBs have lost data in the cloud
- 200% increase in downtime costs from ransomware (1 in 5 businesses infected)
- Natural disasters only account for 5% of downtime events
  - human error was 22%, hardware failure was 45%

Business Continuity & Disaster Recovery Timeline

Disaster Recovery is a part of Contingency Planning and is relevant to BCP



Active Learning Exercise: ALE

- **Let's walk through a scenario:**

You are the owner of an automotive parts manufacturing plant. You rely on robots to do most of the work. The system that manages the robots crashes as a result of a power flicker caused by a storm outside. It is night-time and your night manager does not know how to fix the software. The on-call technician is not answering his/her phone.

- Reference the timeline on the previous slide. At which points in the scenario would you be implanting your various contingency plans? Feel free to add details to the scenario as the timeline progresses.

Business Continuity Planning (BCP)

Why have a BCP? Some numbers to consider…

According to research data kept at the National Archives & Records Administration in Washington, DC:

- Nearly 90% of all small businesses don't have a continuity plan in place
- Only 43% of businesses suffering a disaster ever recover sufficiently to resume business
- Of those that do reopen, only 29% are still operating two years later
- 93% of businesses that lost their data-center for more than 9 days filed for **bankruptcy within one year** of the disaster.
- 50% of businesses that found themselves without data management for more than 9 days filed for **bankruptcy immediately**.

Why Doesn't Everyone Plan?

What are the barriers to creating Contingency Plans like a BCP?

- The Human element (we make mistakes)
- The "it's not going to happen to me" view or philosophy.
  - ex. Insurance policies are not plans…
- We have a tendency to view a disaster as a rarity (low likelihood)
  - "We'll get to it…later…"
- "It hasn't happed yet. And probably never will" (playing the odds?)
- Not on a manager's list of goals – considered someone else's responsibility
- "Looks too BIG! Where would we even start?"
- "We can't afford the personnel or the time to do this!" or "No one has this skillset."

Business Continuity Plan – Controls & Objectives

(taken from ISO 27001)

Information security aspects of BCM

- **Objective**: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Including information security in the BCM process

- A managed *process shall be developed and maintained* for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.

Business continuity and risk assessment

- Events that can cause interruptions to business processes shall be **identified**, along with the **probability** and **impact** of such interruptions and their **consequences for information security.**

Broad BCP objectives

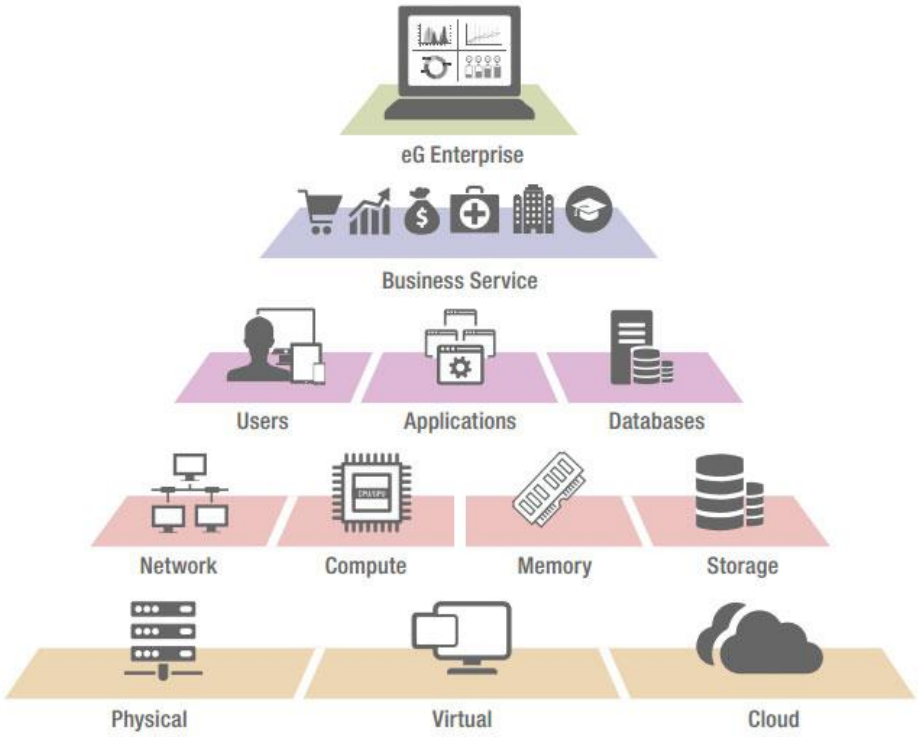
Create, document, test, and update a plan that will:

- Allow **timely** recovery of critical business operations
- Minimize loss ($$)
- Meet legal and regulatory requirements

- ***Availability*** – ***the main focus***
- ***Confidentiality*** – still important
- ***Integrity*** – still important

Scope of BCP

- Used to be just the data center when it started out
- Now includes all aspects of the **IT environment**. **What does that include?**
  - Distributed operations
  - Personnel
  - Network infrastructure
  - Power
  - Environmental controls
  - Telecommunications
  - IoT
  - Wireless



https://www.eginnovations.com/unified-monitoring

BCP Scope – what should your plan consider? (1/2)

- Policy Statement.
- General Introduction and Overview.
- Functional Areas Priorities.
- Critical Resources / Non-critical Resources.
- Procedural Considerations.
- Emergency and Evacuation Procedures.
- Recovery Teams.
- Recovery Processes.
- Emergency Operations Center/Command Center.
- Facility Considerations.
- Inventory Considerations.

BCP Scope – what should your plan consider? (2/2)

- Equipment Considerations.
- Communication Considerations – ex. who talks to the media?
- Documentation Considerations.
- Data/Software Considerations.
- Transportation Considerations.
- Supporting Equipment.
- Responding to the disaster.
- Resume critical business functions.
- Resume Non-Critical Business Functions.
- Planning for Return to the Primary Site (Restoration Operations).
- Interfacing with External Groups.

Anatomy of a Business Continuity Plan

- Awareness of **Roles and Responsibilities**
  - Who will do what? Employees and staff are critical. Pandemic is an extreme example of a disaster where employee resources will be very limited!
- Defined **recovery time objectives**
- **Risk Management** to identify & reduce risks
- Alternate Processes (telecommuting, distance learning)
- Alternate recovery locations
- Off-site storage of critical media *and* non-media items
- Written plans, reviewed & updated regularly
- Frequent plan exercises – **"Iteration Results In Improvement"**

Creating a BCP

- Is an on-going process, not a project with a beginning and an end
  - Creating, testing, maintaining, and updating
  - “Critical” business functions may evolve
- **The BCP team – Who should be on it?**
  - must include both business and IT personnel

- Requires the support of senior management

BCP Policy

Brief introduction to policy:

- Policy is to business as Laws are to society!
- Like the law, policies *maintain order*

i.e. follow it or there may be consequences! Policy is primarily driven by the "people problem"

Three levels of policy:

1. Enterprise Information Security Policy (EISP) e.g. a strategic document.
2. **Issue** Specific Security Policy (ISSP) e.g. BCP.
3. **System** Specific Security Policy (SSSP) e.g. operating a firewall, harden an Operating System, etc.

Business Continuity **Policy Statement** Includes

1. First a Policy statement is needed. (why do you need this policy, what does it cover?)
2. Then the objectives of the policy (what the policy hopes to accomplish)
3. Then the audience (who does this policy apply to or affect?)
4. Then the context (past reviews, document history, etc)
5. Responsibilities and Delegations (who has to do what to meet policy objectives?)
6. Monitoring, evaluation and reporting requirements
7. Policy owner (who to contact if you have questions about the policy)

Document Development – what goes into a policy?

All documentation intended to comply with ISO standards must include all of the following components.

- **Name** of document, version and classification (policy, standard, procedure etc.)
- Document **Owner** – the contact for document content questions and document revisions.
- **Objective** – the purpose of the document
- **Scope** – identifying to whom and/or to what assets the standards and process apply
- Document **Approver** – who gives that document the power to be considered binding?
- **Effective** Date – date the document was implemented and enforced.
- **Last Reviewed** Date – date the document was last reviewed for changes, updates, or document retirement and amendment history.

https://www.fanshawec.ca/sites/default/files/legacy/oldfanshawe/sites/default/files/assets/policies/pdf/a130.pdf

FANSHAWE

COLLEGE POLICY MANUAL

Policy No. & Title: **A130: STUDENT CODE OF CONDUCT**
Policy Sponsor: Executive Director, Student Success
Reference Cttee: College Council
Effective: 2019-11-27
Next Review: 2024-11-27
Approvals: 1990-10-12/CC-90-02; 1996-12-04/SA-96-03; 1997-05-28/CC-96-08; 1998-12-16/CC-98-04; 2003-09-01/CC-02-04; 2008-08-01/CC-07-05; 2010-11-17/CC-10-03; 2012-01-18/CC-11-03; 2013-03-20/CC-12-06; 2019-11-27/CC-19-03

1. PURPOSE

The purpose of the Student Code of Conduct (the Code) is to define the general standard of non-academic conduct expected of students, to provide examples of conduct that may be subject to disciplinary action or restorative measures by the College, to set out the actions that may be imposed, and to describe the disciplinary procedures that the College will follow. The Code seeks to balance student success with the well-being of the College Community by encouraging participatory processes, informal resolution and restorative measures when appropriate.

Community is at the heart of Fanshawe's values. It expresses the connections we have with each other, support we give each other and the respect we show each other.

2. POLICY

Fanshawe College will uphold the Code of Conduct and respond to instances of non-academic student misconduct which may occur both on and off campus and affect the Fanshawe workplace, living, learning and student life environment.

2.1. Principles

2.1.1. In the context of the Code, the goal and responsibility of the College is to provide a learning community encompassing all aspects of college life, such that the pursuit of education and personal growth can take place in a safe and welcoming environment.

2.1.2. The College will identify and respond quickly and effectively to instances non-academic misconduct.

2.1.3. The College and those acting on behalf of the College will ensure that they apply the principles of natural justice and fairness, act in good faith and apply their discretion reasonably.

2.1.4. The College is committed to the respect, inclusion and equality of all persons

2.2. Administration

2.2.1. The Policy Sponsor develops, maintains and implements procedures as are necessary to

What are some of the policy elements in this document?

FANSHAWE

COLLEGE POLICY MANUAL

Policy No. & Title: A130: STUDENT CODE OF CONDUCT
Addendum: **Standard A: SCOPE AND APPLICATION**
Issued by: Executive Director, Student Success
Effective: 2019-11-27

1. SCOPE OF THE CODE

1.1. In the exercise of its disciplinary authority and responsibility, the College treats students as free to organize their personal lives, behaviour, and associations, subject to all local, municipal, provincial, and federal laws, and the policies of the College, including this Code of Conduct.

1.2. The Code applies to student conduct from admission to a course or program until that person has completed the course or graduated from the program, even though the conduct may occur before classes begin or after classes end. When a complaint has been made against an individual for behaviour that was alleged to have occurred while the individual was a student, the individual is deemed a student for the purposes of the Code until the complaint and appeal process is complete.

1.3. Nothing in this Code should be construed to limit freedom of expression as provided by law, provided such activities are orderly, do not disrupt College operations, and do not unreasonably interfere with the right of other members of the College Community to use and enjoy the College's learning, living, and working environment and facilities.

1.4. Whenever appropriate, the College encourages informal resolution of Minor Misconduct.

1.5. Professional organizations and associations affiliated with specific College programs may have standards of behaviour or a specific code of ethics that students may be responsible to understand and with which they are required to comply. Any violations of such standards will be dealt with in accordance with the professional organization or association. Where breach of such standards is also a breach of this Code of Conduct, the student may be subject to disciplinary sanctions under this Code as determined by the Code of Conduct Coordinator (CCC).

Extract from Business Continuity Planning Policy

Maintenance and Assessment

All business continuity plans at The Company must be reviewed at regular intervals to ensure that they are up-to-date and effective. A re-assessment of the threats and risks related to business activities must take place periodically. Plans should be assessed to determine their effectiveness and adjustments made to maintain plans at an effective level. Examples of changes that should trigger a review are included below (but are not comprehensive);

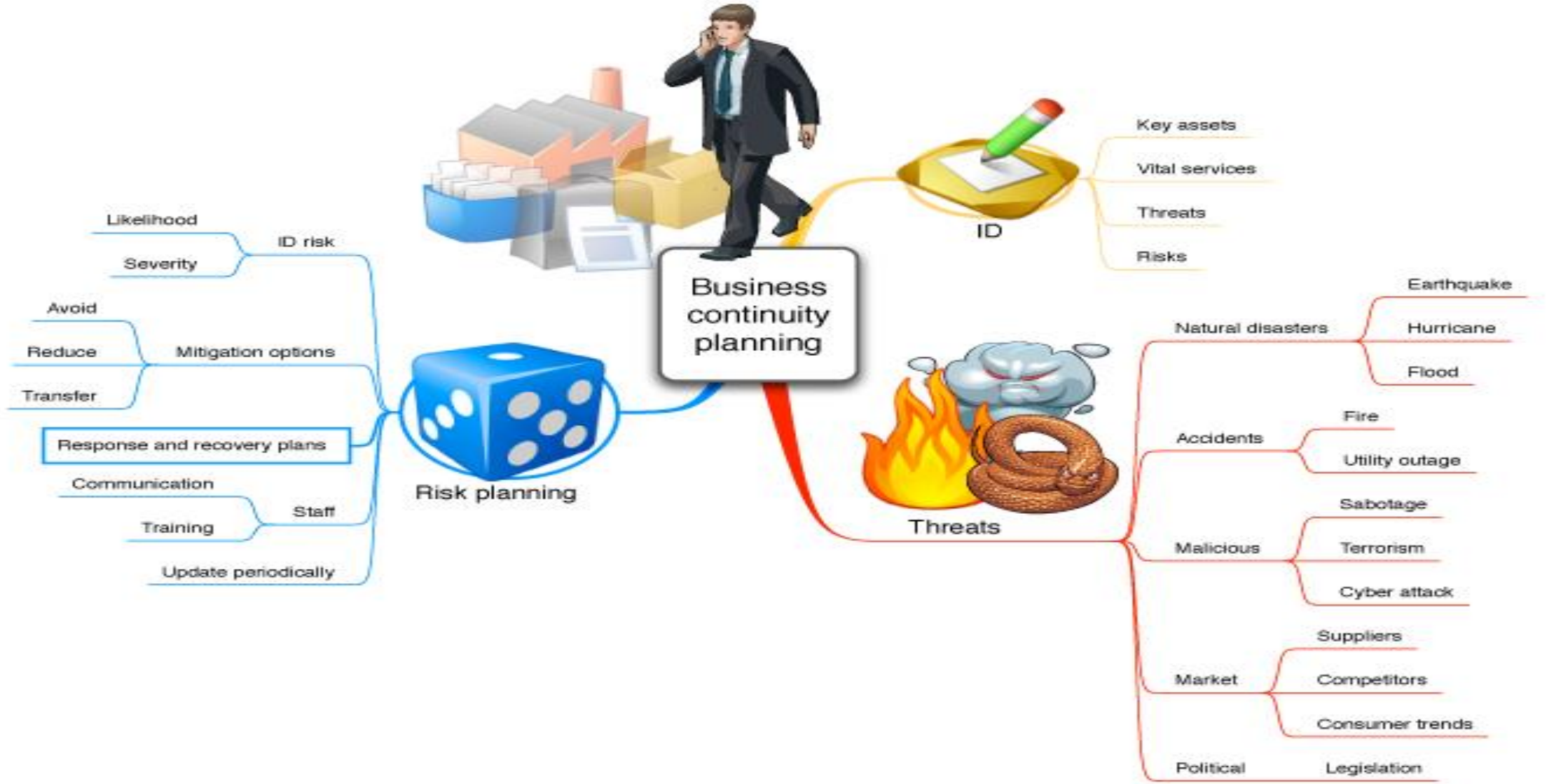
- changes in personnel
- change of location of a system
- changes to legislation
- change of contractors, suppliers or customers
- changes to processes
- changes to technology
- changes to operational or financial risk

Ex. The policy may require a 1-3 year formal review cycle

BCP Team Members

(draw on the expertise across many areas of your company)

- Senior management. (gives binding authority to the group and the plan)
  - "sanctioned and supported"
- BCP planner/coordinator.
- CSIRT (Comp Sec IRT) or Recovery team members.
- **Business unit representatives.**
- Crisis management team.
- **User community.**
- Systems and network experts.
- Information security department.
- **Legal representatives.**


Business continuity planning
ID
Key assets
Vital services
Threats
Risks
Risk planning
ID risk
Likelihood
Severity
Mitigation options
Avoid
Reduce
Transfer
Response and recovery plans
Staff
Communication
Training
Update periodically
Threats
Natural disasters
Earthquake
Hurricane
Flood
Accidents
Fire
Utility outage
Malicious
Sabotage
Terrorism
Cyber attack
Market
Suppliers
Competitors
Consumer trends
Political
Legislation

Five Phases of BCP

FANSHAWE

The five BCP phases

1. Project **initiation**
2. Business Impact Analysis (**BIA**)
3. Develop **recovery strategies**
4. Plan design, development, and **implementation**
5. Testing and monitoring (also includes maintenance, awareness, training)

1. Project Initiation

- Establish **need**. Do you NEED to do this?
- Get **management support/sanction**
- Identify strategic internal and external **resources**.
- Establish **team leads** (functional, technical, management, BCC – Business Continuity Coordinator)
- Create work **plan** (scope, goals/milestones, methods, order/timeline)
  - What if milestone isn't met?
- Prepare and present an initial **Project Report** to management
- Obtain management approval to proceed.
- Develop formal meeting schedules (and stick to them regardless of absences)

2. Business Impact Analysis (BIA)

- The BIA is a management-level analysis that identifies the impact should a potential outage occur.
- Goal: obtain **formal agreement with senior management** on the MTD for each time-critical business resource
- MTD – Maximum tolerable downtime, also known as MAO (Maximum Allowable Outage). https://cloud.google.com/architecture/disaster-recovery
- *Quantifies* loss due to business outage (financial, extra cost of recovery, embarrassment)
- Does not consider what types of incidents cause a disruption; only identifying consequences. Cause is less relevant to the BIA – **consequences are key**.

- Question – what if we have a hybrid or cloud structure how does MTD work?

2. BIA - Purpose

- Provide written documentation to understand the impact associated with possible outages.
- Identify an organization's business functions/assets and determine how critical those functions/assets are to the organization.
- Identify any concerns that staff or management may have (Talk to people, but be wary of answers…)
- Prioritize critical systems.
- Analyze the **impact of an outage**.
- Determine recovery windows (remember RTO?) for each business function.

2. BIA - Procedure

- Choose information gathering methods (surveys, **interviews**, software tools).
- Select interviewees.
- Customize questionnaire.
- Analyze information.
- **Identify time-critical business functions**.
  - Assign maximum tolerable downtimes (MTDs).
  - Rank critical business functions by MTDs.
- Document, prepare, and report recommendations.
- Obtain management approval.

2. BIA - Sample Question Topics for Interviews

- Business function.
- Date of interview.
- Contact name.
- Business process.
- Financial impacts.
- Operational impacts.
- Legal obligations.
- Damage to reputation.
- Technological dependence.
- Interdependencies.
- Existing BCP measures.
- Alternate processing options.
- Customized options:
  - Financial impact
  - Operational impact
  - Legal obligation
  - Damage to reputation

3. Recovery strategies

- Recovery strategies are based on MTDs
- Strategies should be predefined
- Different technical strategies
- Different costs and benefits
- Management-approved (to make sure you have the budget and resources you need)

How to choose which recovery strategies are appropriate?

- Careful cost-benefit analysis
- Driven by business requirements

3. Recovery strategies

Strategies should address recovery of:

- Business operations
- Facilities & supplies
- Users (workers and end-users)
- Network, data center (technical)
- Data (off-site backups of data and applications)
  - Hot site, warm site, cold site, mobile site, timeshares, service bureaus, mutual aid agreements
  - There is a cost for everything! Is it worth it? How do you determine this?

3. Recovery strategies

Technical recovery strategies – subscription service sites and Backups

- Hot, Warm, Cold, Mirror, Mobile

Technical recovery strategies - scope

- Data center
- Networks

Telecommunications Technical recovery strategies – methods

- Subscription services
- Mutual aid agreements
- Redundant data centers
- Service bureaux

Critical Business Function Categories

Item	Required Recovery Time
Very High (1)	0 – 12 hours
High (2)	12 – 24 hours
Moderate (3)	24 - 72 hours
Low (4)	> 72 hours

Item	Required Recovery Time
Nonessential	30 days
Normal	7 days
Important	72 hours
Urgent	24 hours
Critical/Essential	1 – 4 hours

These times may be determined by your risk assessment!

4. Plan Development and Implementation

- Detailed plan for recovery
  - Business & service recovery plans
  - **Maintenance** – your plan WILL degenerate over time. Guaranteed.
  - Awareness & **training**
  - **Testing**
    - Some strategies: desk check, structured walkthrough, simulation, parallel testing, full-interruption testing

4. Plan Development and Implementation

- Sample plan phases
  - Initial disaster response
  - Resume critical business ops
  - Resume non-critical business ops
  - Restoration (return to primary site)
  - Interacting with external groups (customers, media, emergency responders)

4. Plan Development and Implementation - Steps

1. Determine management concerns and priorities.
2. Determine planning scope.
3. Establish outage assumptions.
4. Define prevention strategies for risk management, physical security, information security, insurance coverage, and how to mitigate the emergency.
5. Identify resumption strategies for mission-critical applications and systems at alternate sites.
6. Identify recovery strategies for non-mission-critical applications and systems at alternate sites and for relocating the emergency operations center/command center to the recovery site.

4. Plan Development and Implementation - Steps

7. Develop service function recovery plans, including information processing, telecommunications, etc.
8. Develop business function recovery plans and procedures.
9. Develop facility recovery plans.
10. Identify the response procedures.
11. Gather data required for plan completion.
12. Review and outline how the organization will interface with external groups. (Communication)
13. Review and outline how the organization will cope with other complications beyond the actual disaster.

5. BCP final phase

- Testing
- Maintenance
- Awareness
- Training

5. BCP final phase – Plan Testing

- **Until it's tested, you don't have a plan**
- Kinds of testing:
  - Structured walk-through: step-by-step review of the BCP by functional reps who meet together – no one is actually walking anywhere ☺
  - Checklist - similar to SWT but checklists are distributed to business units, who review the checklists individually
  - Simulation - kind of like "war games" – simulation stops at point where equipment would be relocated
  - Parallel - DR site is put into full operation without taking down the primary – results compared between the two
  - Full interruption - Full-scale test of BCP by a planned fail-over to the secondary site and fail-back to the primary. Also called a "simulation" if a sandbox or hot site is used.
- **Note**: more than one kind of test may be useful. For instance, a simulation and a parallel test complement each other.

5. Goals of Plan Testing – why do we test the plan?

- Demonstrate that output performance of backup systems and networks are consistent with production systems and networks.
- Adapt and update existing plans to encompass new requirements.
- Test all components of the plan, including hardware, software, personnel, data and voice communications, procedures, supplies and forms, documentation, transportation, utilities, alternate site processing, etc.

5. Plan Maintenance

- Resolve all problems/deficiencies found during testing.
- Implement change management.
- Audit and address audit findings
- Build maintenance procedures into the organization operation.
- Annual review of plan
- Centralize responsibility for updates.
- Report updates regularly to team members and, if necessary, to senior management.
  - Fix problems found in testing
  - Implement change management
  - Audit and address audit findings
  - Annual review of plan
  - Build plan into organization

5. Training!!

- BCP team is probably the DR team.
- All staff should be trained in the business recovery process.
- Training should cover a range of outcomes, from simple awareness of the major provisions of the plan to the ability to carry out specific procedures.
- BCP training must be on-going and scheduled
- Training needs to be part of the standard on-boarding and part of the corporate culture.
- Consider **coverage** and **cross-training**! Who is covering for whom?

- How often do disasters occur?
- How good are people at executing procedures that they don't use very often?
- How do you ensure something is part of the corporate culture when it's designed to deal with an event we hope never happens?

5. Training on Communication

- Communication is critical
- Employees, customers, business partners must know key information about your plan if your plan is to work.
- Plans must be periodically reviewed in team meetings and shared with new team members.
- Contact information for all team members must be current (use contact lists on mobile devices!)

Communication Plans must include:

- **Clear chains of authority**
- **Clear listing of tasks, roles and responsibilities**
- **Methods of communication:**
  - **Mobile phones? Portable radios? Hand signals ☺**
- **Standing meetings (times, numbers)**
- **Alternate meeting locations**
- **Centralized communication point (web site, etc…)**

Secret Plans won't work! The more people who know the more likely your plan will be followed

FANSHAWE

You Need to consider Off-Site Storage!

When a facility is lost or inaccessible, all items inside are no longer available. What is needed in off site storage if you had to recover from scratch

- PC backup media must be stored off-site – "Remote" Backup
- Critical, non-media, documents and materials must be available in an off-site location, accessible by appropriate individuals or teams during a disaster or exercise.
- Key personnel must know where off-site storage items are located and to where items will be shipped (Hot-site, Incident Command Center or remain in off-site storage?)

Effective BCP Is Built On 7 P's

- **Program** - the total BCM strategy
- **People** - Roles and responsibilities, H&S, awareness and education
- **Processes** - all organisational processes including ICT
- **Premises** - buildings & facilities
- **Providers** - supply chain inc. outsourcing
- **Profile** - brand, image and reputation
- **Performance** - benchmarking, evaluation & audit

Common Pitfalls In BCP

Pitfalls Plans can be ...	Description
Incomplete	The BCP process is not complete. Outputs such as the business continuity plan and policy either do not exist or exist in incomplete form.
Inadequate	The plan and strategies can't deal with the level of risk that the organization deems acceptable.
Impractical	The plan is not practical or achievable within the organization's constraints (manpower, time, and budget, for example).
Overkill	The plan is overly elaborate or costly with respect to the overall level of business risk that the organization is willing to take.
Uncommunicated	The business continuity team has not communicated the plan to all the right people. Staff—both management and technical—remains unaware of business continuity issues.
Lacking a defined process	Business continuity processes remain ill defined. Staffers are unsure of how to react in a failure scenario, or they discover too late that their existing processes fall short.
Untested	The organization hasn't tested its plan, or hasn't tested it thoroughly enough to provide a high level of confidence in its soundness.
Uncoordinated	The business continuity effort lacks organization and coordination. The organization has either not established a business continuity team, or the team lacks individuals who can effectively drive the effort to completion.
Out of date	The plan hasn't been reviewed or revised in light of changes in the organization, its business, or technology.
Lacking in recovery thinking	The organization doesn't adequately address how it intends to recover to a fully operational state after executing its business continuity plans.

References and Reminders

- Computer Security – Principles & Practices, 3rd Edition (by William Stallings)
- Management of Information Security (by M Whitman)
- ISO27000 series of Standards

Reminders

1. Your second written assignment (10%) will be posted this week (due in week 8)
2. Consider contributing to the discussion forum. Bonus marks make a difference!
3. Next week we will finish discussing BCM and DRP, as well as start talking about **Data Protection and Restoration**