CE/CZ 4064
Security Management

Contingency Planning & Management
Contingency

- Chance favours the prepared mind - Louis Pasteur

contingency
/kənˈtɪndʒəni/ 

noun

a future event or circumstance which is possible but cannot be predicted with certainty.
"a detailed contract which attempts to provide for all possible contingencies"
synonyms: eventuality, (chance) event, incident, happening, occurrence, juncture, possibility, accident, chance, emergency; More

- a provision for a possible event or circumstance.
"stores were kept as a contingency against a blockade"

- an incidental expense.
"allow an extra fifteen per cent on the budget for contingencies"
Contingency plan

- Used for managing risk
- Business, Government
- To cope with **catastrophic circumstances** that render normal operations infeasible
- tsunami, terror attack, ...
Why contingency planning?

- Bad things are often unpredictable but inevitable

The economics of Information Security: We'll ship it on Tuesday and get it right by version 3

No perfect system: “Failures in complex systems are inevitable, regardless of the care of operation and the redundancy of safety mechanisms.” – Charles Perrow

Emergence: A cascade of events: e.g. from a tsunami to a nuclear reactor melt down …
Why contingency planning?

- The show must go on

“customers should be able to view and add items to their shopping cart even if disks are failing, network routes are flapping, or data centers are being destroyed by tornados”

- Amazon in their Dynamo systems paper
Natural disasters
Human errors
Cyber (attacks)
Tech failures

impacting

Availability
Reliability
Resiliency
Recoverability
etc.

resulting

IT system
disaster

Source: http://archive.fortune.com/magazines/fortune/twintowers/
If you want business continuity then you can’t continue with IT as business as usual

"Many companies maintained their systems under the basic idea that they could reconstruct the systems with only minor interruption to the enterprise," said Keith Payne, IT security officer at Javitch, Block & Rathbone, a law firm with offices in Ohio and three other states.

Losses of technology and intellectual property on "such a large scale" were considered unlikely before 9/11, Payne said.

"Before 9/11, our customers did not heavily evaluate the possibility that the entire firm could cease to exist with no pre-indicators," he said. "We have made large investments in identifying all assets in the scope of how they contribute to the overall ability to operate. No longer are the days of backup tapes being moved off-site weekly; now mirrored systems are maintained with geographical separation."
Technological solutions
Technological solutions

New solutions also bring along new risks!
Threat of catastrophic cyber-incidents on organizations

Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
Crisis

Crisis event:
Has the potential to have many knock-on and long term adversarial effects, affecting reputation, stock prices, etc.

“The great test lies not in the crisis itself but in the ways we respond.”

- Steve Forbes
Forward in The Communicators: Leadership in the Age of Crisis
Multiple response paradigms

**Emergency:** Something time critical which needs quick response to reduce damage/losses of people’s life, physical or information assets

**Crisis:** A situation with potential knock-on and long term adversarial effects, affecting reputation, stock prices/market, etc.

**Disaster:** Involves loss of physical assets and/or people’s life/health, and/or critical IT systems
Multiple response paradigms

“customers should be able to view and add items to their shopping cart even if disks are failing, network routes are flapping, or data centers are being destroyed by tornados.” - Amazon

Business continuity

“Business Continuity Management (BCM) is broadly defined as a business process that seeks to ensure organizations are able to withstand any disruption to normal functioning.” - Elliott, Dominic and Herbane, Brahim
Contingency planning is a process through which businesses develop a strategy to deal with unanticipated events that would impede daily activities or normal operations.” – Cynthia A Scarinci
Business continuity management

Emergency Response
- Time critical
- Initial control of emergency situation
- Save human life
- Stabilizing, security, damage assessment

Crisis Management
- Strategic direction/policy issues
- Crisis communications (media management)
- External liaison
- Service recovery coordination

Business Recovery
- Phased recovery of business-critical processes/services
- Disaster Recovery
  - Recovery of infrastructure & services
  - Returning to “business as usual”

Multiple responses but shared purposes
29th Sept 2014: The HKMA released a statement earlier today: “In view of the public order situation in Central and other areas, HKMA and affected banks have activated their business continuity plans this morning to maintain the normal operations of the core functions of the banking system. The Currency Board mechanism will maintain the stability of the Hong Kong dollar exchange rate. The HKMA will also inject liquidity into the banking system as and when necessary under the established mechanism.”
Given that **BCPs involve a cost**, this raises the question of what is the worst case scenario that AIs should plan for. This is an extremely difficult question on which to advise and institutions will to some extent need to form their own judgement. However, it would seem sensible for AIs to plan on the basis that they may have to **cope with the complete destruction of buildings in which key offices or installations are located** (rather than just denial of access for a period) and the **loss of key personnel** (including senior management).

Regulatory requirements

Example: Hong Kong Monetary Authority

AIs should avoid placing excessive reliance on external vendors in providing BCP support, particularly where a number of institutions are using the services of the same vendor (e.g. to provide back-up facilities or additional hardware).

Staff should be told clearly where they should go in an emergency, how do they get there and what do they do when they get there.

AIs should establish a well-defined command centre structure and guidance should be given to staff as to how to communicate with the command centre in an emergency.

AIs should examine the extent to which key business functions are concentrated in the same or adjacent locations and the proximity of back-up sites to primary sites. Key facilities should be sufficiently distanced to avoid being affected by the same disaster (e.g. they should be on separate telecommunication networks and power grids). The systems at back-up sites should be maintained and upgraded together with those in the primary sites. Recovery capacity may need to cater for processing volumes that exceed normal levels if, for example, more inquiries need to be handled.

To cater for the fact that other parties may be affected by a disaster, AIs should periodically test the ability of their back-up sites to communicate with the back-up sites of key counterparties, customers and service providers.

There should be clear procedures in the BCP indicating how and in what priority vital records are to be retrieved or recreated in the event they are lost, damaged or destroyed.

AIs' BCPs should address the issue of how to handle media and PR issues to maintain public confidence in the event of disaster.
Drivers

- Beyond operational security
- To cope with circumstances that render normal operations infeasible
- Regulatory requirements & guidelines, e.g., NIST 800-34 (Contingency Planning Guide for Federal Information Systems)

*In addition to technical considerations, Information Systems Contingency Planning is guided by Internal Agency & Government wide mission and business drivers.*

Business continuity planning

**HOW?**

1. **Conduct BIA and RA** (Business impact analysis & risk analysis)
   - Establish business recovery priorities, timescales, & minimum requirements

2. **BC Strategy Formulation**
   - Options for meeting priorities, timescales & minimum requirements, & recommendation

3. **BC Plan Production**
   - Plans, organization, responsibilities, logistics, detailed action tasklists

4. **BC Plan Testing**
   - Test strategy, test plans, testing, and evidence

5. **BC Awareness**
   - Awareness for all staff

6. **Ongoing BCP Maintenance**
   - Ongoing maintenance activities

---

**RISK REDUCTION**

As early as 2004, IDA and the Singapore IT Standards Committee established the world’s first standard for BC/DR service providers – the SS507. The standard specifies **stringent requirements that service providers must possess in order to provide a “trusted” operating environment**. SS507 subsequently became one of the **base documents for the ISO/IEC 24762 Guidelines** for ICT DR Services which was published in January 2008.

**Reference:** ISO/IEC 24762:2007 – ICT Disaster Recovery Services
Business continuity management

basic components
- Policy
- People with defined roles & responsibilities
- Management processes
- Documentations
- BCM processes

Business continuity management systems (BCMS) standard
Business continuity management

Business continuity management systems (BCMS) standard
PDCA (plan–do–check–act or plan–do–check–adjust) is an iterative four-step management method used in business for the control & continuous improvement of processes and products. It is also known as the Deming circle/cycle/wheel, Shewhart cycle, control circle/cycle, or plan–do–study–act (PDSA).

Business continuity management systems (BCMS) standard
## Contingency plans & controls
For FISMA from NIST

### TABLE D-8: SUMMARY — CONTINGENCY PLANNING CONTROLS

<table>
<thead>
<tr>
<th>CNTL NO.</th>
<th>CONTROL NAME</th>
<th>WITHDRAWN</th>
<th>ASSURANCE</th>
<th>CONTROL BASELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>LOW</td>
<td>MOD</td>
<td>HIGH</td>
</tr>
<tr>
<td>CP-1</td>
<td>Contingency Planning Policy and Procedures</td>
<td></td>
<td></td>
<td>x x x x</td>
</tr>
<tr>
<td>CP-2</td>
<td>Contingency Plan</td>
<td></td>
<td></td>
<td>x x x x</td>
</tr>
<tr>
<td>CP-2(1)</td>
<td>CONTINGENCY PLAN</td>
<td>COORDINATE WITH RELATED PLANS</td>
<td></td>
<td>x x</td>
</tr>
<tr>
<td>CP-2(2)</td>
<td>CONTINGENCY PLAN</td>
<td>CAPACITY PLANNING</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-2(3)</td>
<td>CONTINGENCY PLAN</td>
<td>RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS</td>
<td></td>
<td>x x</td>
</tr>
<tr>
<td>CP-2(4)</td>
<td>CONTINGENCY PLAN</td>
<td>RESUME ALL MISSIONS / BUSINESS FUNCTIONS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-2(5)</td>
<td>CONTINGENCY PLAN</td>
<td>CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>CP-2(6)</td>
<td>CONTINGENCY PLAN</td>
<td>ALTERNATE PROCESSING / STORAGE SITE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-2(7)</td>
<td>CONTINGENCY PLAN</td>
<td>COORDINATE WITH EXTERNAL SERVICE PROVIDERS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-2(8)</td>
<td>CONTINGENCY PLAN</td>
<td>IDENTIFY CRITICAL ASSETS</td>
<td></td>
<td>x x</td>
</tr>
<tr>
<td>CP-3</td>
<td>Contingency Training</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-3(1)</td>
<td>CONTINGENCY TRAINING</td>
<td>SIMULATED EVENTS</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>CP-3(2)</td>
<td>CONTINGENCY TRAINING</td>
<td>AUTOMATED ENVIRONMENTS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-4</td>
<td>Contingency Plan Testing</td>
<td></td>
<td></td>
<td>x x x x</td>
</tr>
<tr>
<td>CP-4(1)</td>
<td>CONTINGENCY PLAN TESTING</td>
<td>COORDINATE WITH RELATED PLANS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-4(2)</td>
<td>CONTINGENCY PLAN TESTING</td>
<td>ALTERNATE PROCESSING SITE</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>CP-4(3)</td>
<td>CONTINGENCY PLAN TESTING</td>
<td>AUTOMATED TESTING</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-4(4)</td>
<td>CONTINGENCY PLAN TESTING</td>
<td>FULL RECOVERY / RECONSTITUTION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-5</td>
<td>Contingency Plan Update</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>CP-6</td>
<td>Alternate Storage Site</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-6(1)</td>
<td>ALTERNATE STORAGE SITE</td>
<td>SEPARATION FROM PRIMARY SITE</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>CP-6(2)</td>
<td>ALTERNATE STORAGE SITE</td>
<td>RECOVERY TIME / POINT OBJECTIVES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-6(3)</td>
<td>ALTERNATE STORAGE SITE</td>
<td>ACCESSIBILITY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-7</td>
<td>Alternate Processing Site</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-7(1)</td>
<td>ALTERNATE PROCESSING SITE</td>
<td>SEPARATION FROM PRIMARY SITE</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>CP-7(2)</td>
<td>ALTERNATE PROCESSING SITE</td>
<td>ACCESSIBILITY</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>CP-7(3)</td>
<td>ALTERNATE PROCESSING SITE</td>
<td>PRIORITY OF SERVICE</td>
<td></td>
<td>x x</td>
</tr>
<tr>
<td>CP-7(4)</td>
<td>ALTERNATE PROCESSING SITE</td>
<td>PREPARATION FOR USE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP-7(5)</td>
<td>ALTERNATE PROCESSING SITE</td>
<td>EQUIVALENT INFORMATION SECURITY SAFEGUARDS</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>CP-7(6)</td>
<td>ALTERNATE PROCESSING SITE</td>
<td>INABILITY TO RETURN TO PRIMARY SITE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NIST 800-34 r1 (2010)  
NIST 800-53 r4 (2013)
Organizational considerations

Orchestrating BC

- Who should be responsible for BCM?
- De/Centralized planning and execution
- Stakeholders’ roles and responsibilities
- Reporting line
- Resourcing
- Planning vs Recovery organizations

Reference: Goh Moh Heng
Managing Your Business Continuity Planning Project
Business Impact Analysis

1. **Determine Critical Business Processes, Services, and Products**
   Those that must be restored immediately after a disruption to ensure the affected firm’s ability to protect its assets, meet its critical needs, and satisfy mandatory regulations and requirements.

2. **Identify activities that support provision of critical business processes, services, and products**

3. **Assess impacts over time of not performing these activities**
   e.g., Loss of life, damage to physical assets, denial or disruption of critical technology services, etc.

4. **Set prioritized timeframes for resuming these activities**
   e.g., Minimum acceptable level; Maximum tolerable downtime

5. **Identify dependencies and supporting resources for these activities, including all third parties dependencies**
Business Impact Analysis

Determine Critical Business Processes, Services, and Products

Ten Critical Components

Our plans to ensure business continuity address the ten key areas FINRA and NYSE stated must be addressed:

1. Data back-up and recovery (hard copy and electronic) – identification of the location of primary books and records (hard copy and electronic) and the location of back-up books and records (hard copy and electronic). In addition, firms must be prepared to describe how they back up data, as well as how they will recover data in the event of a significant business disruption.

2. All mission critical systems – systems that are necessary, depending on the nature of a member's business, to ensure prompt and accurate processing of securities transactions, including, but not limited to, order taking, order entry, execution, comparison, allocation, clearance and settlement of securities transactions, the maintenance of customer accounts, access to customer accounts and the delivery of funds and securities.

3. Financial and operational assessments – written procedures that allow a firm to identify changes in its operational, financial, and credit risk exposures. Operational risk focuses on the firm's ability to maintain communications with customers and to retrieve key activity records through its "mission critical systems." Financial risk relates to the firm's ability to continue to generate revenue and to retain or obtain adequate financing and sufficient equity. Firms may also face credit risk (e.g., where its investments may erode from the lack of liquidity in the broader market), which would also hinder the ability of the firm's counter-parties to fulfill their obligations.

4. Alternate communications between customers and firm – alternate means of communications that a firm will use to communicate with its customers in the event of a significant business disruption.

5. Alternate communications between firm and its employees – alternate means of communications that a firm will use to communicate with its employees in the event of a significant business disruption.

6. Alternate physical location of employees – alternate locations must be designated for employees, including key personnel that have been identified to assist in the resumption of business operations.

7. Critical business constituents, banks, and counter-party impact – effect a significant business disruption will have on a firm's relationship with its critical business constituents, banks, and counter-parties, and how it will deal with those impacts.

8. Regulatory reporting – available means a firm can use to continue its compliance with regulatory reporting requirements.

9. Communications with regulators – communication with regulators through whatever means are still available, including the telephone, fax, email, and the Internet.

10. Providing customers prompt access to their funds and securities – measures a firm will use to make customer funds and securities available to customers in the event of a significant business disruption.

Functions and shared services that could be critical:
Deposit taking; Lending & Loan servicing; Payments, clearing, custody & settlement, Wholesale funding markets, Capital markets & investment activities; Finance-related & Operational shared services

Sources:
https://www.db.com/en/content/Business-Continuity-Program.htm
BIA: Key considerations

MTD: Maximum Tolerable Downtime

Also known as Maximum Tolerable Period of Disruption (MTPD)
Period of time after which an organization’s viability will be irrevocably threatened if delivery of a particular product or service cannot be resumed.
MTD drives the selection of the recovery strategy and schedule.

- Policy and Regulatory Compliance Requirement
- Customer impact analysis
- Third party dependencies
- System impact analysis
- Recovery requirements
Recovery Requirements

**Recovery Time Objective (RTO)**

RTO is the duration of time, from the point of disruption, within which a system should be restored.

Defined for different activities and is always shorter than MTD

**Recovery Point Objective (RPO)**

RPO refers to the acceptable amount of data loss for an IT system should a disaster occur.
BCM and DRP practices focus on shortening period of disruption and reducing the impact of an incident by risk mitigation and recovery planning.
Considerations
Recovery strategy

- **Type of disaster**
- **Points of impact**
- **Depth & Scope of impact**
- **Availability of resources**

**Scenario driven**
- Different scenarios may require different strategy and solutions
Recovery options

**Common approaches**
- Hot, cold, semi-hot sites (data center, workspace, war rooms, operating centers, call centers, etc.)
- Shared services/mutual support arrangements (internal and/or external)
- Work from home arrangement (with remote access)

**Amortize resources**
- Use of Virtualization
- Use of third party cloud services
- Re-purposing of existing services
Third party dependencies

Outside Service Providers (OSP)
- Who should be responsible for BCM?
- What’s their MTD, RPO, RTO?
- Alternative solutions
- Joint exercises
- Cost and SLA implications

Correlations
- What are their contingency plans should similar incident is also impacting them?
- Multiple organizations’ dependency on single DR provider.
Plan development

Specific BCP for each business and support functions, with prioritization based on criticality of services/products/processes

Steps to consider

- Incident notification and assessment
  Triggers for plan activation

- Communication plan

- Authority to activate plan (primary & secondary)

- Awareness and training plans and schedule

- Testing/rehearsal/exercising plans and schedule

- Maintenance plan

- Budget requirements
Incident response structure

Detection & Notification

- Monitoring and alerting capabilities
- Internal & external communication systems (receiving national or regional risk advisory)
- Reliability and redundancy of communication systems
- Documentation – journaling/recording of activities and information received/sent

Incident response

- Establish, document, and implement procedures and a management structure to respond to disruptive incidents
- Leveraging existing incident management structure, including physical security, environmental safety, information security, and other related teams
- With necessary responsibility, authority, and competence to manage an incident.
- Budget requirements
Crisis communication

Timeliness

- Use social media as means for mass communication with large audience?
- Risks of abuse & miscommunication exacerbating the situation
- Spokesperson/trained PR personnel
- Pre-established partnership with channels like media
Use well vetted BCMP tools

**BCMP components**
(a non-exhaustive list)

- Risk assessment for availability
- BIA from loss of people, IT, facilities, suppliers
- Business process & IT dependency mapping
- Workflow management
- Analytics for understanding effectiveness, risk reduction & cost
  - etc

Reference: Gartner report
ICT Readiness for Business Continuity (IRBC)

ICT readiness is an essential component for many organizations in the implementation of business continuity management and information security management. As part of the implementation and operation of an information security management system (ISMS) specified in ISO/IEC27001 and business continuity management system (BCMS) respectively, it is critical to develop and implement a readiness plan for the ICT services to help ensure business continuity.

Reference: ISO/IEC 27031
Plan activation

Triage
- False or true incident?

Notification
- Team members
- Possible incident

Escalation
- Incident confirmed

Damage assessment
- Can it be contained?
- Growing severity?

Declaring a disaster
- Executive notification

Mobilization of response team
- Permanent & virtual teams
Concluding remarks

**Summary**

- Contingency planning is key to business continuity
- Different responses, but shared purposes
- Top-down and bottom-up supports and commitments are both critical
- No perfect plan – but several standards & guidelines – needs to constantly test, update, communicate, test, ... (PDCA: plan, do, check, act)

if everything else fails ...