Business Continuity Management and Crisis Management and Role of Internal Auditors

Prepared and presented by: Mr. Ibrahim Alfaifi

Saturday 21 March, 2020
Agenda of this awareness session

✓ What is Business Continuity? Its importance and requirements
✓ Business Continuity Management (BCM) lifecycle
✓ Business Continuity Plan and Disaster Recovery Plan
✓ Emergency Response and Crisis Management
✓ Business Continuity Common Concerns and Challenges
✓ How Internal Auditors can “Add Value” to the BCM Program?
Business Continuity Plan (BCP)
خطة استمرارية الأعمال

Disaster Recovery Plan (DRP)
خطة التعافي من الكوارث

Emergency Response
الاستجابة للطوارئ

Crisis Management
إدارة الأزمات

Business Impact Analysis (BIA)
تحليل الأثر على الأعمال

Recovery Time Objective (RTO)
هدف وقت الاسترجاع

Recovery Point Objective (RPO)
هدف نقطة الاسترجاع

Recovery Period
فترة التعافي

Restoration Period
فترة الاستعادة

Risk Assessment (RA)
تقييم المخاطر

Maximum Acceptable Outage (MAO)
أقصى انقطاع مقبول
Hope For The Best
Plan For The Worst

Jack Reacher
قرار مجلس الوزراء رقم (87) وتاريخ 7/ 2 / 1440 هـ بشأن إنشاء (مجلس المخاطر الوطنية)
برئاسة سمو ولي العهد

- إجراء تقويم شامل للمخاطر الوطنية
- إنشاء «مركز التميز» لنشر ثقافة إدارة المخاطر
- دعم الجهات المعنية، لنشر الوعي العام بالمخاطر
- إنشاء «مركز إدارة الكوارث والأزمات»
- دراسة وإعلان رفع مستوى الجهوزية ضد المخاطر
- إعداد حلول لمراقبة المخاطر ومتابعتها
<table>
<thead>
<tr>
<th>Risk and threat assessment — past twelve months</th>
<th>Risk and threat assessment — next twelve months</th>
<th>Consequences of disruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health incidents replace IT as the leading cause of disruption over the past twelve months</td>
<td>Cyber-attacks remain at the top of the future threats risk index. The disconnect continues between previous incidents vs perception of future threats</td>
<td>The negative impact on staff wellbeing is of greater consequence than financial loss during a disruption</td>
</tr>
<tr>
<td>Leading causes of disruption over the past 12 months (Risk Index Rating)</td>
<td>Leading causes of disruption over the next 12 months (Risk Index Rating)</td>
<td>Leading impacts or consequences of disruption over the past 12 months</td>
</tr>
<tr>
<td>![Health incident icon]</td>
<td>![Cyber-attack and data breach icon]</td>
<td>![Loss of productivity icon]</td>
</tr>
<tr>
<td>Health incident: <strong>13.9</strong></td>
<td>Cyber-attack and data breach: <strong>6.4</strong></td>
<td>Loss of productivity: <strong>69.3%</strong></td>
</tr>
<tr>
<td>IT and telecom outage: <strong>13.0</strong></td>
<td>IT and telecom outage: <strong>5.4</strong></td>
<td>![Negative impact on staff morale/wellbeing icon]</td>
</tr>
<tr>
<td>Safety incident: <strong>12.0</strong></td>
<td>Extreme weather events: <strong>4.9</strong></td>
<td>Negative impact on staff morale/wellbeing: <strong>42.8%</strong></td>
</tr>
<tr>
<td>Lack of talent/key skills: <strong>11.5</strong></td>
<td>Critical infrastructure failure: <strong>4.7</strong></td>
<td>![Customer complaints received icon]</td>
</tr>
<tr>
<td>Cyber-attack and data breach: <strong>11.2</strong></td>
<td>Lack of talent/key skills: <strong>4.5</strong></td>
<td>Customer complaints received: <strong>41.4%</strong></td>
</tr>
<tr>
<td>![Lack of talent/key skills icon]</td>
<td>![Critical infrastructure failure icon]</td>
<td>![Reputation damage icon]</td>
</tr>
<tr>
<td>![Cyber-attack and data breach icon]</td>
<td>![Extreme weather events icon]</td>
<td>Reputation damage: <strong>39.5%</strong></td>
</tr>
<tr>
<td>![Health incident icon]</td>
<td>![Safety incident icon]</td>
<td>![Loss of revenue icon]</td>
</tr>
<tr>
<td>![IT and telecom outage icon]</td>
<td>![Loss of productivity icon]</td>
<td>Loss of revenue: <strong>36.3%</strong></td>
</tr>
</tbody>
</table>
2019 | Business Continuity Benchmark Study

83% Continuous of Operations

80% Employee Safety

Only 9% Their business continuity programs are ‘very mature’

Key Objectives of BCM Program

66% ROI is not measured for their business continuity program

76% Business Continuity is a priority for top executives in their organization
Top 10 risks in terms of Impact

10. Infectious diseases
Disruption of Electronic Services in 2017

Disruption of mada Payment Services in 2018

Jeddah floods in 2009 affected Saudi Airlines

Mid of 2019

Disruption of mada Payment Services in 2018

Jeddah floods in 2009 affected Saudi Airlines

Mid of 2019
What is Business Continuity?

**Business Continuity** is the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

**BCM** is a holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause. It provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

*(Source: ISO 22313/22301)*
Importance of BCM

• Continue the business operations
• Safeguard assets

High attention to:
• Management Support & Awareness
• BCM Investment
• ROI for BCM investment
• Risk & Audit priority and role
Business Continuity Objectives

- Viability
  - Keeping the company in business
- Earnings/Profit Protection
  - Protecting the Enterprise’s Financial Commitments
- Continuing New Business
  - Preserving the ability to sell in the marketplace
- Brand Protection
  - Avoiding public embarrassment and loss of credibility

People
Data/Info.
Facilities & Equipment
Comm. Infra./IT Sys.
How to deal with an incident/crisis from A-Z
• Build a business Case
• Understand the value
• Establish BCM Program/goals aligned with business goals

• Identify BC disruptive events, threats and vulnerabilities
• Assess the likelihood and impact of disruptive events
• Develop BC risk mitigation strategies

• Identify business processes and define the critical processes
• Define RTO, RPO and resources for each process
• Identify other parties/suppliers and physical resources for recovery

• Define alternative (staffing, sourcing, offices)
• Plan for transition back to normal operations + BCP and DRP
• Select the suitable recovery solutions and recovery sites

• BCM awareness and training
• Maintain the BCM Program and BC Plans
• Exercise and test BC capabilities + Measurement and improvement
Management Commitment and Support

Defining a central group/committee within the organization that is responsible for BCM and managing governance (BC Strategy, Policy, Manual, Working Groups)

Making sure that BCM Program is part of each BU and communicating the importance of BCM (Communication Protocol)

Making sure appropriate investment and funding for organization-wide BCM activities

Participating in BC exercises, training sessions, and other emergency management events
Business Continuity Risk Assessment & Mitigation Plan

**Risk Assessment:** is the process of identifying **internal** and **external threats** and vulnerabilities, identifying the **likelihood** and **impact** of an event arising from such threats or vulnerabilities, defining the controls in place or necessary to reduce exposure and evaluating the cost for such controls.

### Disruptive Events
- Natural disasters (earthquakes, rain/flooding, etc)
- Industrial events (fire, explosions, etc).
- Supplier failures (provider disruptions and electricity utilities)
- Medical epidemic such as a pandemic or other medical risks
- Labor disruption
- Economic or political instability
- Human factors such as employee errors, criminal acts, and fraud
- IT Risks and Cyber Attack

### Assessing the risks
- The BC risk assessment can be used to determine the impact to critical business processes
- Assessing the impact and likelihood of each disruptive event
- Certain factors should be evaluated to understand the scope and the impact of each potential event: Geographic extent of the impact, Days of impact, Availability of staff, Availability of operations/offices, Availability of IT.

### Developing Risk Mitigation Strategies
- Developing and deploying BC risk mitigation strategies will help to minimize the impact of disruptive events and will improve response capabilities.
- Examples:
  - Loss of primary location: arrange for alternative location or initiate work from home policy.
  - Loss of IT: ensure to have a DR
  - Loss of data: ensure you have appropriate data backup to restore
In March 2019, aviation authorities around the world grounded the Boeing 737 MAX passenger airliner after two new airplanes crashed within five months, killing all 346 people aboard.
Business Impact Analysis (BIA): is the process of determining the criticality of business activities and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption.

1. Identify the business processes, activities and key resources
2. Identify the business impact of each process (Financial, Reputational, etc), then determine the process RTO and RPO. Based on identified business impact.
3. Identifying the Other Parties and Physical Resources (other departments, vendors, key equipment and systems, etc).
4. Obtaining Sponsor and Executive Approval for the BIA for each Business Group.

Remark: BIA is valuable input to Audit Universe and IA Annual Assessment.
Recovery Point Objective (RPO): the amount of data that can be lost (loss tolerance).
Recovery Time Objective (RTO): acceptable downtime to recover the service.
Maximum Tolerance Downtime (MTD)/Maximum Acceptable Outage (MAO): is the time frame during which a recovery must become effective before an outage compromises the ability of an Organization to achieve its business objectives and/or survival.
8.2: Business Impact Analysis (BIA) and Risk Assessment

- **8.2.2 Business Impact Analysis**
  - Identifying activities that support the provision of products and services
  - Assessing the impacts over time of not performing these activities
  - Setting prioritized timeframes for resuming these activities
  - Identifying dependencies and supporting resources

- **8.2.3 Risk Assessment**
  - Identify risks of disruption to the organization’s prioritized activities
  - Systematically analyze risk
  - Evaluate which disruption related risks requirement treatment
  - Identify treatments commensurate with business continuity objectives and in accordance with the organization’s risk appetite
KFC Crisis as an example!

Chicken shop without any chicken !!!
Business Continuity and Recovery Strategies

Business recovery and continuity strategies may include some solutions such as:

- Manual processes in case IT systems are down
- IT Disaster Recovery to continue critical IT services
- Alternative facilities (Offices/Work from home, suppliers, etc)
- Alternative staffing (avoid SPOF)
- Outsourcing (Reciprocal agreement, or secondary vendors)

Planning to Transition Back to Normal Operations: A plan must be developed to transition the organization back to a normal state.
BCP and DRP

Documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.

Recovery plan that focuses on recovering the information and communication technology infrastructure (considered as part of BCP).

**Main Content of BCP**

- Purpose and Scope
- Roles and Responsibilities
- Key contacts
- Plan Activation/Deactivation
- Communication
- Physical sites and transportation
- Incident Response
- Recovery Process
- Required Resources
- Restoration plan (back to normal)
BCP and DRP  Cont.

Data Center

Business Continuity Center

IT Disaster Recovery site
Disaster Recovery Site for IT

**Cold site**
- Little or no equipment
- No network connectivity
- Not ready for automatic failover
- No data synchronization
- High risk of data loss
- Cheap

**Warm site**
- Partially redundant equipment
- Network connectivity is enabled
- Failover occurs within hours or days
- Daily or weekly data synchronization
- Minimum data loss
- Cost-effective

**Hot site**
- Fully redundant equipment
- Network connectivity is enabled
- Failover occurs within hours or days
- Near real-time data synchronization
- Zero data loss
- Expensive
• **Crisis Management** is strategic or organization wide incidents where an asset or business continuity incident is escalated as the incident severity increases.

• To have active Crisis Management: it should have (Dedicated Team + Plan + To Be Tested Annually).
2.8 Crisis Management Plan

Principle
The Member Organization should define, approve and implement a crisis management plan that would facilitate a well-managed response for major incidents, including rapid communication to ensure overall safety to both internal and external stakeholders.

Objective
To ensure the Member Organization has effective crisis management plan in place and up-to-date for critical member organization products, services, business functions and processes, in case of a disruptive incident.

Control considerations
1. A crisis management plan should be defined, approved and implemented.
2. The compliance with the crisis management plan should be monitored.
3. The effectiveness of the business continuity program within the crisis management plan should be measured and periodically evaluated.
4. The Member Organization should document a crisis management plan(s) that define(s) how crisis resulting from a major incident(s) will be addressed and managed, and should include at least:
   a. Criteria for declaring a crisis.
   b. The member organization should establish a command center for centralized management and an emergency command center.
   c. Crisis-management team members. Considering representatives of the critical products, services, functions and processes of the Member Organization (including Communications department)
   d. Contact details of those who are part of the crisis management team (including third-parties)
   e. Definition of the steps to be taken during and after a crisis or disaster (including the mandates required)
   f. Communication plan including the media response plan, to address the communication with the internal and external stakeholders during crisis.
   g. The frequency of crisis management tests
BC Awareness, Training, Maintenance and Exercise

**Awareness and Training** on all BCM Program activities should be conducted periodically. Negative lessons learned from testing activities should be included in the BCM training programs.

BCM program should be **Updated & Maintained** in annual basis or after any major change to ensure that RA, BIA and processes and equipment/systems are up to date.

There should be a **Testing Plan** to cover all BCM program activities such as (BCP, DRPs, Crisis Management Plan, Emergency Response Plan, Communication Protocol, etc).
# Business Continuity – Some Types of Exercises

<table>
<thead>
<tr>
<th>Exercise Type</th>
<th>Description and Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desk Check or Plan Audit</td>
<td>Normally involves the plan owner to ensure that plan content is not outdated</td>
</tr>
<tr>
<td>Orientation or Plan Walkthrough</td>
<td>Walk through the document with staff expected to implement the plan to ensure team members understand their new/updated roles</td>
</tr>
<tr>
<td>Tabletop Exercise</td>
<td>Bring the entire BC/CM team together for a session to work collaboratively through a realistic scenario to identify challenges and build rapport in solving them together</td>
</tr>
<tr>
<td>Communication Testing</td>
<td>Testing the communication process/protocol and it involves actually contacting business partners and employees</td>
</tr>
<tr>
<td>Alternate Site Testing</td>
<td>Testing of all restoration/recovery components at an alternate site (either relocate staff to the alternative site or testing the sufficiency and effectiveness of IT assets at the alternate site)</td>
</tr>
<tr>
<td>End-to-end Testing</td>
<td>Testing the capability of both business and IT</td>
</tr>
</tbody>
</table>
Cyber Resilience

Cyber resilience is the ability to prepare for, respond to and recover from cyber attacks.

1. Manage and protect
   - Malware protection
   - Information and security policies
   - Formal information security management programme
   - Identity and access control
   - Security teams are competent and receive regular training
   - Security staff awareness training
   - Encryption
   - Physical and environmental security
   - Patch management
   - Network and communications security
   - Systems security
   - Asset management
   - Supply chain risk management

2. Identify and detect
   - Security monitoring
   - Active detection

3. Respond and recover
   - Incident response management
   - ICT continuity management
   - Business continuity management
   - Information sharing and collaboration

4. Govern and assure
   - Comprehensive risk management programme
   - Continual improvement process
   - Governance structure and processes
   - Board-level commitment and involvement
   - Internal audit
   - External certification/validation
Some Security Controls During BC Activities

- Security requirements and controls should be included within BC activities/offices
- Logical, physical and environmental security controls
- IT DR should have security controls as the primary Data Center.
- Data backup security

- Two-factor authentication for systems, emails, etc
- Hard desk encryption for laptop/devices
- Restricting data to be transferred
- Awareness (confidentiality, working in secure place/avoiding public Wi-Fi, not sharing password, social engineering attack “phishing messages”, etc)
- Avoid using public derive to store organization’s sensitive information
- Enabling software for data backup
How Internal Auditors can “add value” to the BCM Program?
Coronavirus (COVID-19) as an example:

In the Face of the Coronavirus, Internal Auditors Must Do More Than Don Masks (2\textsuperscript{nd} March, 2020)

By Richard Chambers, President and CEO of The IIA

1) Understand and assess the full range of immediate risks
2) Assess the organization's existing crisis management and business continuity plans
3) Advise your organization on thinking beyond immediate risks (social engineering, phishing attacks)
4) Advise your organization on thinking about the long-term implications
5) Continue to monitor and update your thinking (being agile)
Coronavirus (COVID-19) as an example: Cont.

**CAN THE POWER OF PRAYER ALONE STOP A PANDEMIC LIKE THE CORONAVIRUS? EVEN THE PROPHET MUHAMMAD THOUGHT OTHERWISE | OPINION**

CRAIG CONSIDINE
ON 3/17/20 AT 1:06 PM EDT

• إذا وقع الطاعون بأرض فلا تخرجوا منها، وإذا وقع بأرض ولست بها فلا تهبطوا ... ما يسمى علمياً (الحجر المنزلي)
  النظافة من الإيمان

• الفعل بالأسباب و الأخذ بالإجراءات الاحترازية، قصة صاحب الجمل، (اربطوا جملكم أولآً، ثم ثقوا بالله)
• التداوي والفاعل بالأسباب للعلاج، إن الله لم يضع داء إلا وضع له شفاء إلا داء واحد .. الهرم
• غسل اليدين قبل الأكل
What is the **BCM Maturity Level** in your Organization?
BCM Common Concerns and Challenges

1. BCM Program Maintenance and Update
2. Business Continuity Plans Testing
3. Scope Coverage of Business Continuity (limitation in the investment)
4. Prioritization Business Processes and the integration between all processes
5. Appointing the wrong person to lead BCM Program (BCM Program Ownership)
6. Communications (with employee, vendors/suppliers, clients, regulator, management, etc)
7. Security Controls during recovery operations
8. Declaring the crisis to the public
9. Updating the IT infrastructure in the IT DR site to reflect the setup of the primary IT site
What Internal Auditors should do?

Before Crisis
- RA & BIA as input to audit plans
- Be an “observer” member in BCM activities
- Check regulatory requirements
- Evaluate the adequacy of:
  - Mgt. support and commitment
  - BCM strategy, governance, policy and procedures/manual
  - BCM training and awareness
  - BCM test results

During Crisis
- Be an “observer” member in the testing activities
- Evaluate the adherence to the BCM plans:
  - Executing the BCP and DRP
  - Effectiveness of Response, Recovery and Restoration
  - How the Crisis is managed
  - Communication effectiveness

After Crisis
- Lesson learned and improvements plan to BCM program
- Evaluate the effectiveness of BCM Program
- Alignment with Business RTOs and RPOs
- Provide recommendations to enhance the BCM Program activities
BCM Resources and Certifications

SAMA Business Continuity Framework, 2017
13 Sections  75+ Controls
الأسئلة والاجابة على استفساراتكم ..

تمنياتي للجميع بالتوفيق، ودوام الصحة والعافية ..

@i_alfaifi
alfaifi
ibrahimalfifi@gmail.com