การบริหารความต่อเนื่องทางธุรกิจ
Business Continuity Management

โครงการอบรมผู้บริหารเทคโนโลยีสารสนเทศระดับสูง CIO รุ่นที่ 25

21 มกราคม 2558

อภิชัย พงษ์โพธากุล CISA, CISM, CRISC

Speaker’s profile

อภิชัย พงษ์โพธากุล

คุณอภิชัย ปัจจุบันดำรงตำแหน่ง ผู้อำนวยการ ฝ่ายบริหารความเสี่ยงของตลาดหลักทรัพย์แห่งประเทศไทย รับผิดชอบในการสนับสนุนคณะอนุกรรมการบริหารความเสี่ยง และฝ่ายจัดการ ในการดูแลและติดตามความเสี่ยงขององค์กร เพื่อให้เกิดความมั่นใจว่าการบริหารความเสี่ยงองค์กรของกลุ่มตลาดหลักทรัพย์เป็นไปอย่างมีประสิทธิภาพ เกิดการพัฒนา และมีการปฏิบัติงานด้านการบริหารความเสี่ยงทั่วทั้งองค์กรในทิศทางเดียวกัน และเป็นไปตามมาตรฐานที่ดีตามแนวปฏิบัติสากล

นอกจากนี้ คุณอภิชัย ยังมีประสบการณ์มากกว่า 15 ปี ในองค์กรที่ปรึกษาธุรกิจ โดยมีประสบการณ์ในการตรวจสอบเทคโนโลยีสารสนเทศ และการให้คำปรึกษาด้านการบริหารความเสี่ยง การจัดทำแผนความต่อเนื่องทางธุรกิจ การปรับปรุงกระบวนการปฏิบัติงาน และวางระบบบัญชี เป็นต้น

ประวัติการศึกษา

- วิทยาศาสตรมหาบัณฑิต สาขาการบริหารเทคโนโลยี (Technology Management) วิทยาลัยนวัตกรรมอุดมศึกษา มหาวิทยาลัยธรรมศาสตร์
- บัญชีบัณฑิต สาขาเทคโนโลยีสารสนเทศทางการบัญชี (Accounting Information System) คณะพาณิชยศาสตร์ และการบัญชี จุฬาลงกรณ์มหาวิทยาลัย

Professional Certifications

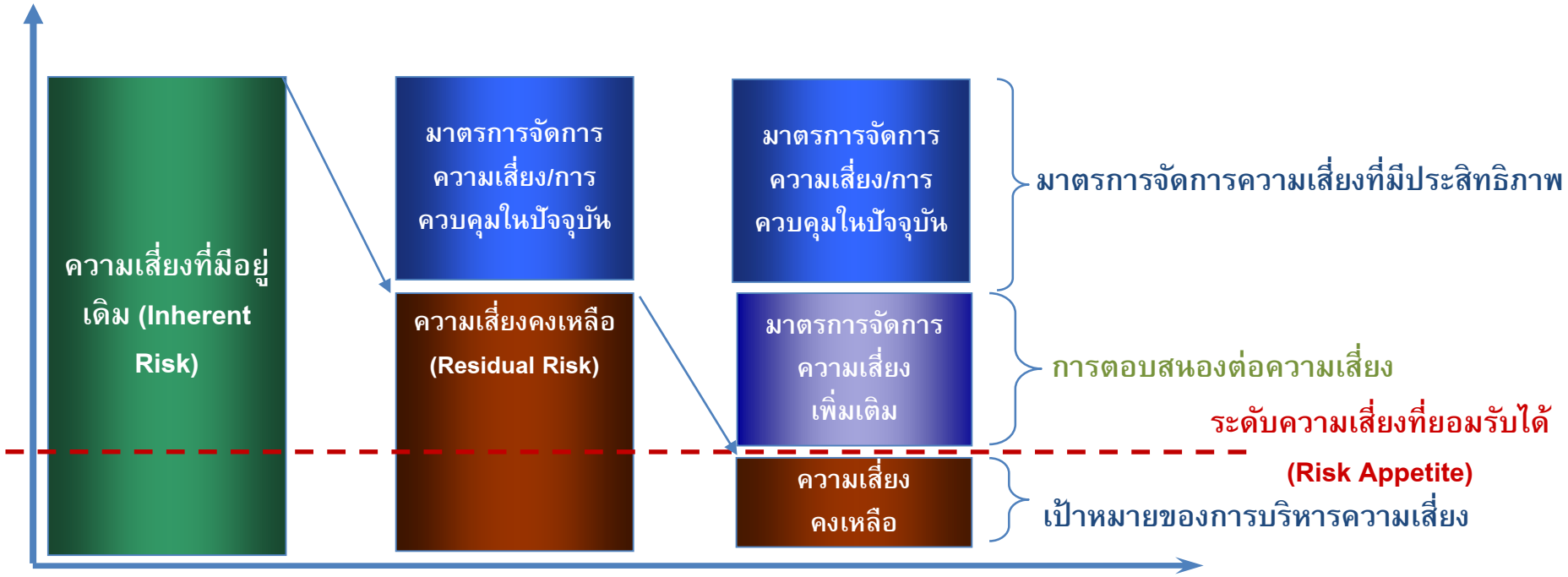
- Certified Information Systems Auditor (CISA), USA
- Certified Information Security Manager (CISM), USA
- Certified in Risk and Information Systems Control (CRISC), USA

หัวข้อการบรรยาย

1. วัตถุประสงค์ของการบริหารความต่อเนื่องทางธุรกิจ
2. แนวทางการพัฒนาระบบการบริหารความต่อเนื่องทางธุรกิจ
3. กรณีศึกษาเรื่องการบริหารความต่อเนื่องทางธุรกิจ
4. ผลสำรวจด้านการบริหารความต่อเนื่องทางธุรกิจ

1. วัตถุประสงค์ของการบริหารความต่อเนื่องทางธุรกิจ

หลักการบริหารความเสี่ยงองค์กร



TREAT

การจัดการความเสี่ยง – พิจารณากำหนดมาตรการเพิ่มเติมในการลดความเสี่ยง เช่น การออกนโยบายหรือมาตรการใหม่ การจัดทำโครงการ

TERMINATE

การหยุดความเสี่ยง – พิจารณายกเลิกกิจกรรมที่ทำให้เกิดความเสี่ยง โดยการหยุดดำเนินการ หรือเปลี่ยนแปลงวิธีการดำเนินการใหม่ เป็นต้น

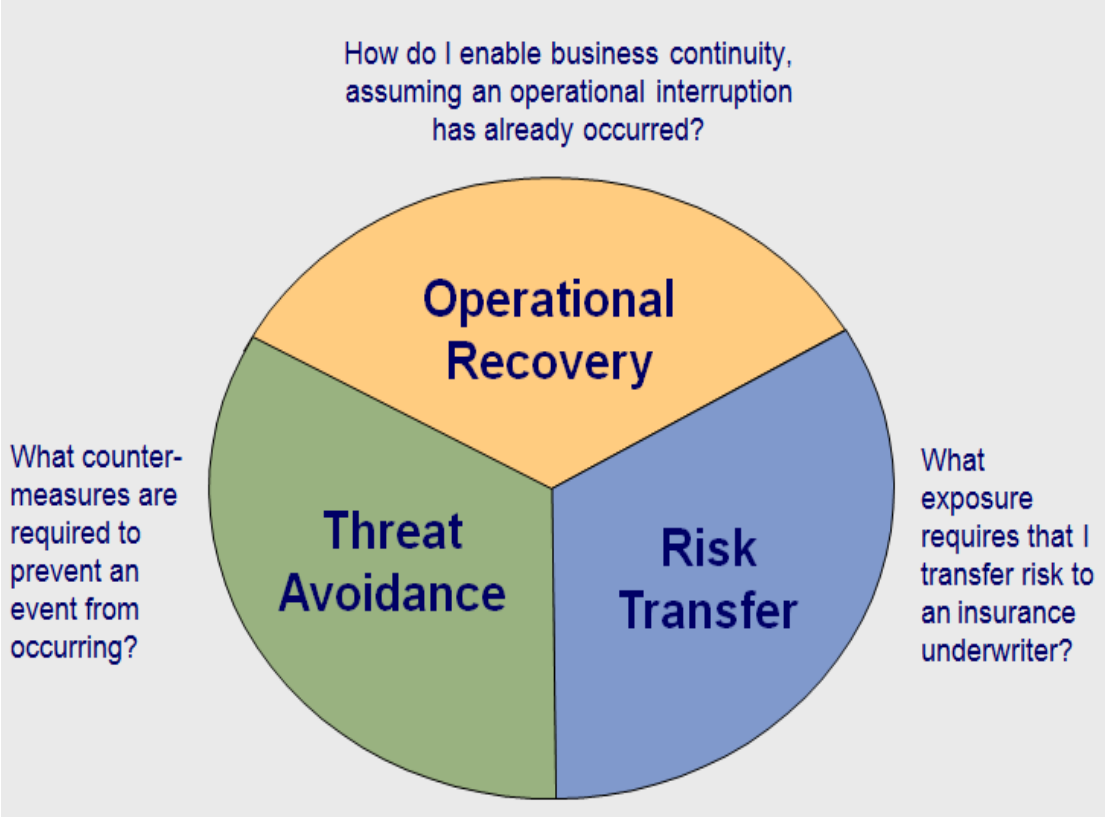
TRANSFER

การถ่ายโอนความเสี่ยง – พิจารณาถ่ายโอนความเสี่ยงไปยังหน่วยงานที่เกี่ยวข้องเพื่อจัดการความเสี่ยงร่วมกัน หรือถ่ายโอนไปยังหน่วยงานภายนอก เช่น การว่าจ้าง หรือการทำประกัน

TAKE

การยอมรับความเสี่ยง – พิจารณายอมรับความเสี่ยงและดำเนินกิจกรรมที่มีความเสี่ยง โดยกำหนดให้มีการติดตามความเสี่ยงอย่างใกล้ชิด

การเชื่อมโยง BCM สู่การบริหารความเสี่ยงองค์กร

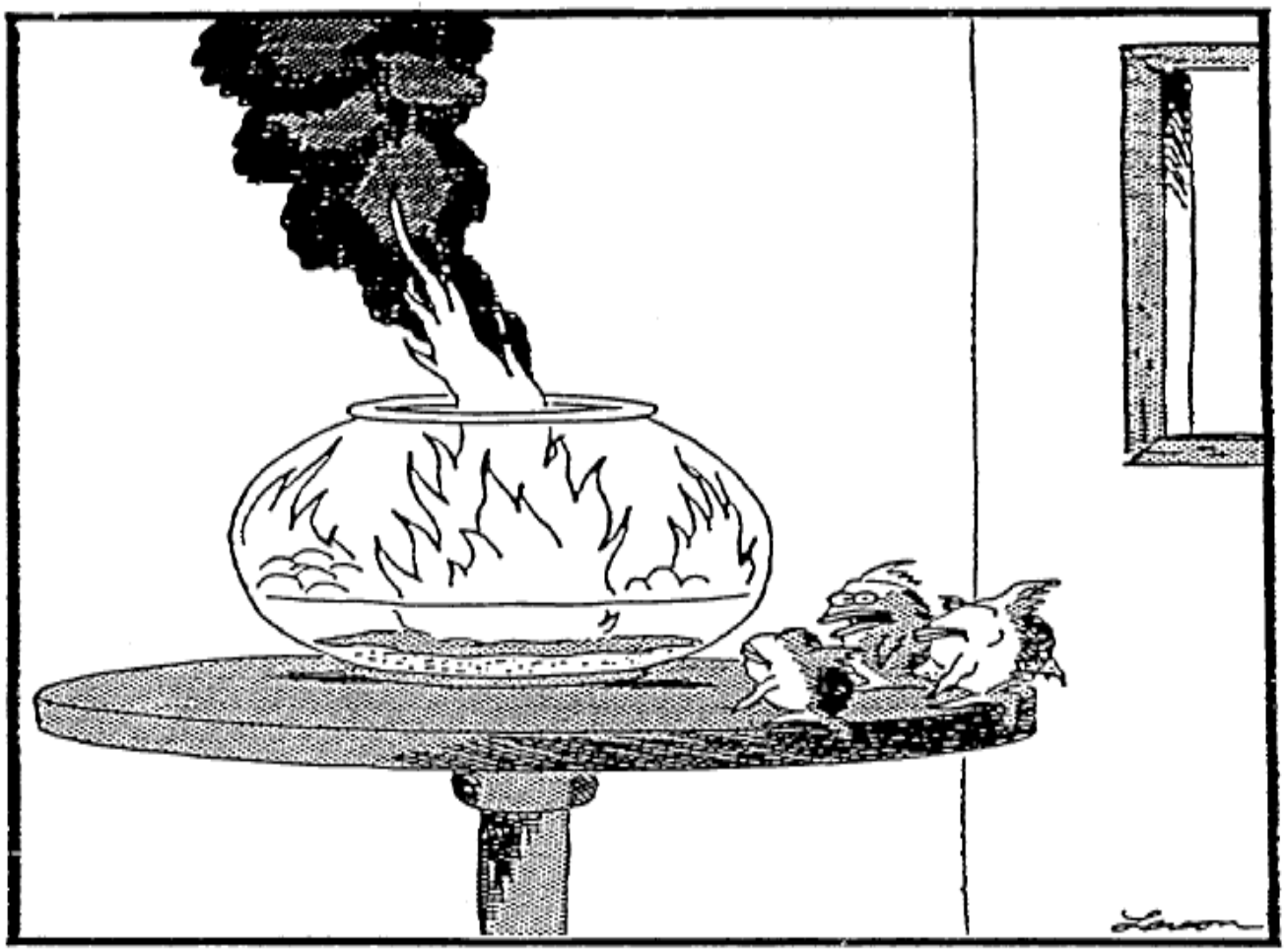


Source: Business Continuity Planning and Enterprise Risk Management, John Phelps

การเชื่อมโยง BCM สู่การบริหารความเสี่ยงองค์กร จะช่วยทำให้องค์กรสามารถบริหารจัดการต้นทุนการดำเนินงานได้อย่างมีประสิทธิภาพ

“ผู้บริหารสามารถใช้ผลจากการวัดระดับความเสี่ยงที่มีผลกระทบสูงถึงสูงมากแต่มีโอกาสเกิดขึ้นน้อยมาพิจารณาจัดทำแผนความต่อเนื่องทางธุรกิจ”

Don’t get caught without a plan



"Well, thank God we all made it out in time.
...'Course, now we're equally screwed."

ทำไม BCM ถึงมีความสำคัญกับความสำเร็จขององค์กรในปัจจุบัน?

"Maintaining business operations in the event of disruption is of utmost importance to your business's profitability."

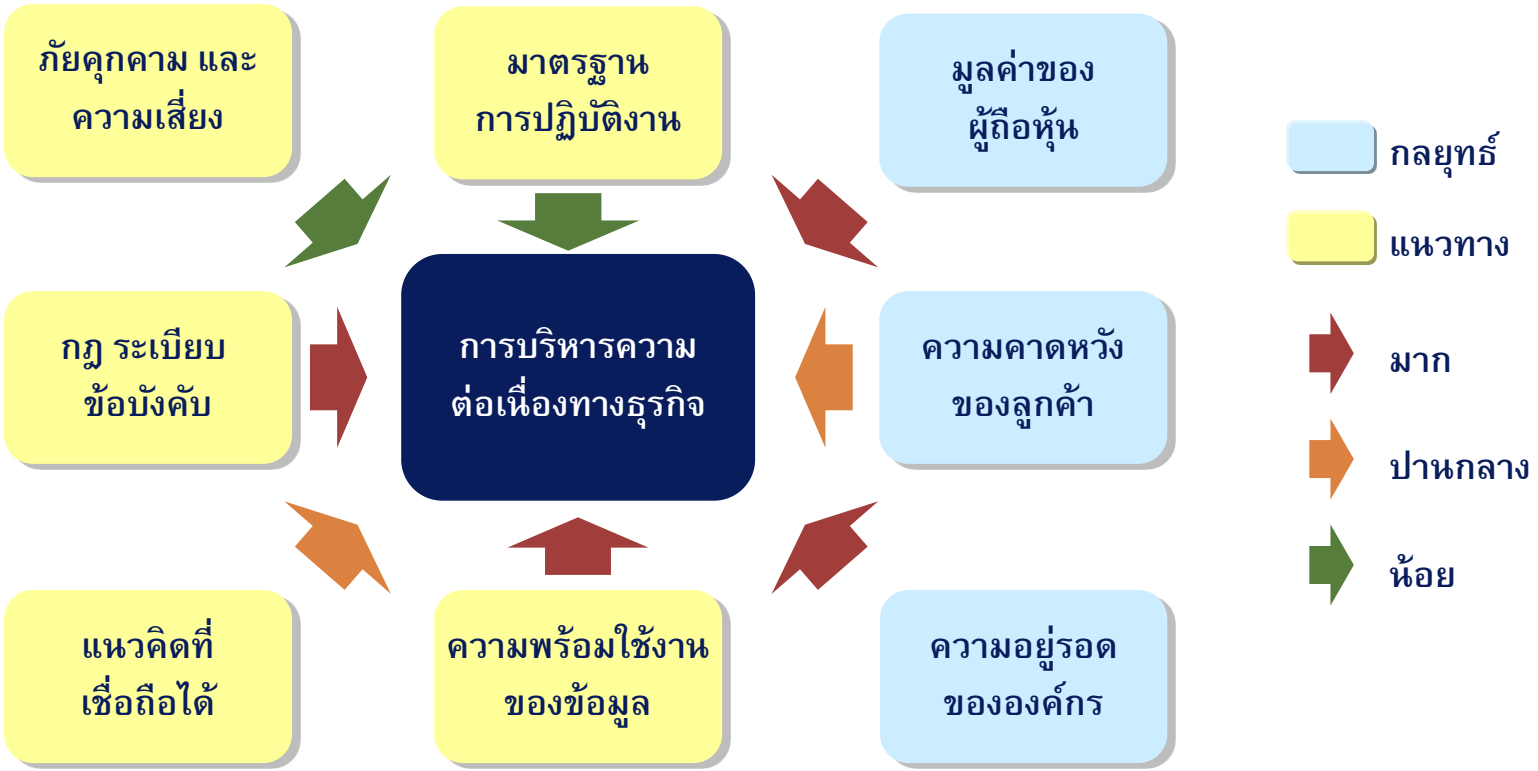
Source: BSI Thailand

"Achieving ISO 22301 certification demonstrates our commitment to providing a reliable high quality service to our customers. It shows that resources, investment and processes in place to protect ourselves from potential service disruption therefore minimizing impact on our customers."

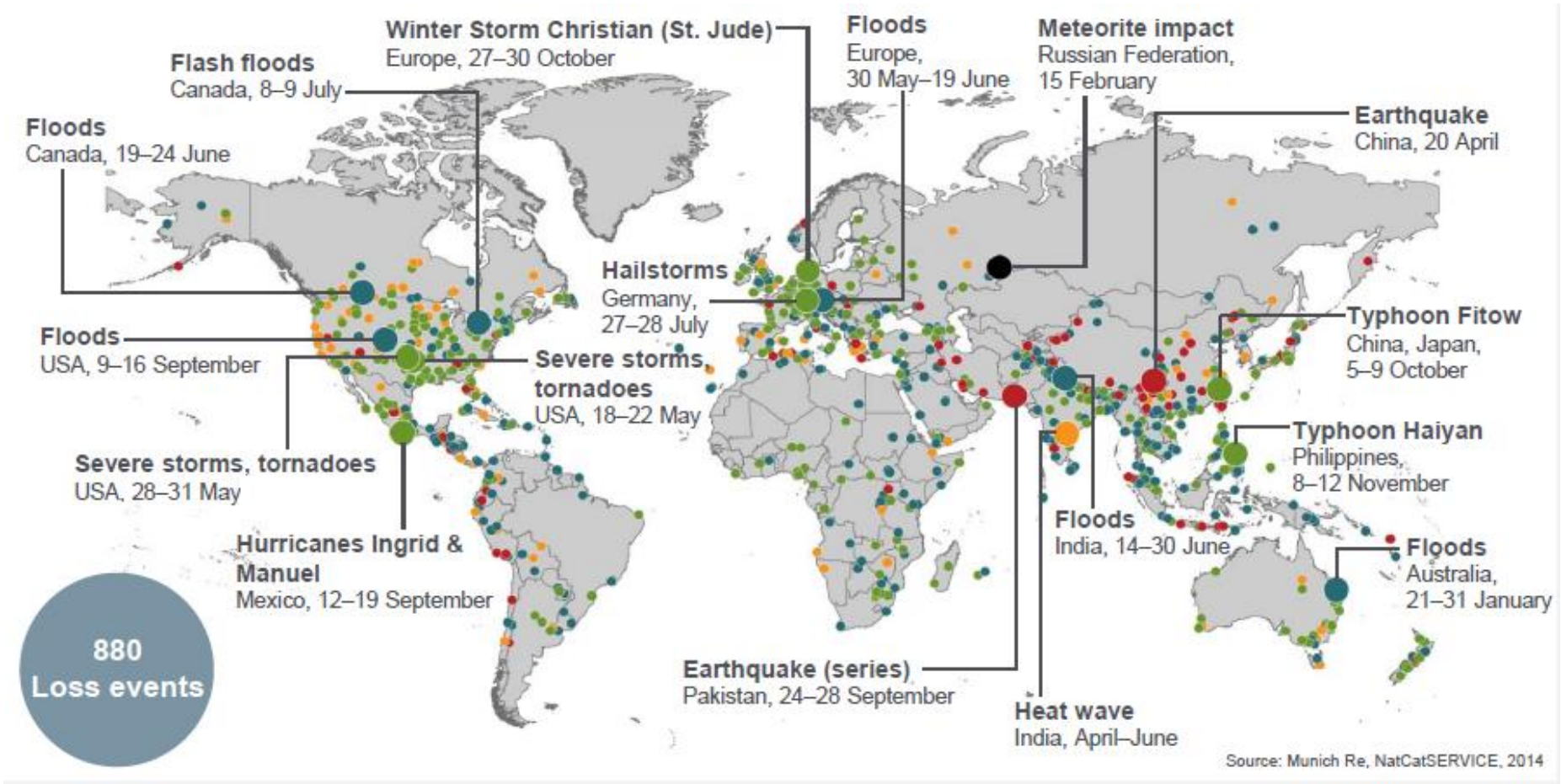
Derek McManus
CCO and Board BC Champion,
Telefónica UK Limited

แรงขับเคลื่อนในการจัดทำโครงการบริหารความต่อเนื่องทางธุรกิจขององค์กร

การบริหารความต่อเนื่องมิใช่เพียงการจัดการเกี่ยวกับภัยธรรมชาติที่เกิดขึ้น หากแต่ขึ้นอยู่กับปัจจัยและความต้องการด้านกลยุทธ์เป็นสำคัญด้วย ในขณะที่จำนวนของภัยธรรมชาติและหายนะที่เกิดขึ้นจากมนุษย์ได้เพิ่มขึ้นเรื่อยๆ กฎ ระเบียบ ข้อบังคับ ความคาดหวัง และความต้องการในแต่ละธุรกิจก็เป็นตัวขับเคลื่อนให้แต่ละองค์กรต้องมีการเตรียมตัวในการบริหารจัดการกับเหตุขัดข้องต่างๆ ที่เกิดขึ้น



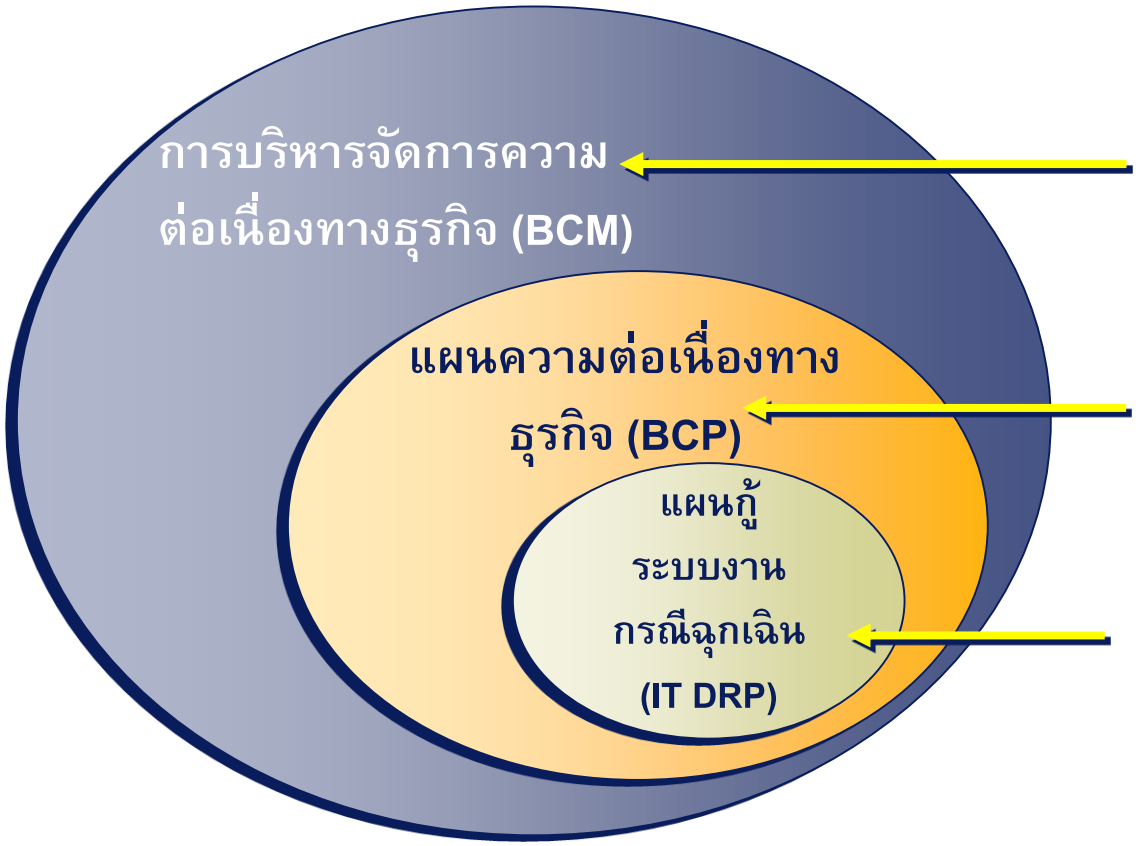
2013 World Catastrophic Events



- Natural catastrophes
- Selection of significant Natural catastrophes
- Geophysical events (earthquake, tsunami, volcanic activity)
- Meteorological events (storm)
- Hydrological events (flood, mass movement)
- Climatological events (extreme temperature, drought, wildfire)

Source: Munich Re, NatCatSERVICE 2014

การบริหารจัดการความต่อเนื่องทางธุรกิจ (BCM)



กระบวนการบริหารจัดการความต่อเนื่องทางธุรกิจ

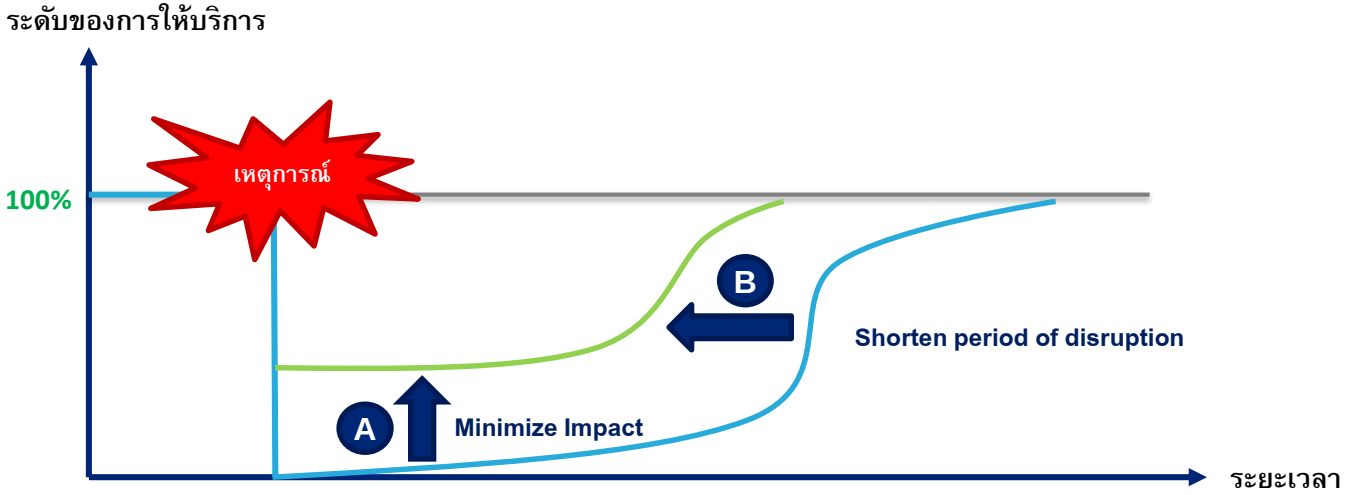
เน้นการกอบกู้กระบวนการทางธุรกิจหลักที่สำคัญ

เน้นการกอบกู้ระบบสารสนเทศที่ใช้สนับสนุนกระบวนการทางธุรกิจหลัก

BCM คืออะไร

BCM คือ องค์รวมของกระบวนการบริหารซึ่งชี้บ่งภัยคุกคามต่อองค์กร และผลกระทบของภัยคุกคามนั้นต่อการดำเนินธุรกิจ และให้แนวทางในการสร้างขีดความสามารถให้องค์กรมีความยืดหยุ่น เพื่อการตอบสนองและปกป้องผลประโยชน์ของผู้มีส่วนได้ส่วนเสีย ชื่อเสียง ภาพลักษณ์ และกิจกรรมที่สร้างมูลค่าที่มีประสิทธิผล

มอก. 22301 - 2553



วัตถุประสงค์หลัก

A. เกิดผลกระทบต่อองค์กรน้อยที่สุด (Minimize Impact)

> การวางแผนและเตรียมการรองรับเพื่อลดระดับผลกระทบและความเสียหายจากเหตุการณ์ให้น้อยที่สุด

B. กลับมาดำเนินธุรกิจหลักภายหลังการหยุดชะงักได้เร็วที่สุด

> ดำเนินการตามแผนเพื่อให้สามารถกลับมาดำเนินงาน / ให้บริการได้เร็วที่สุด

> กำหนดระยะเวลาในการกู้คืนกระบวนการทางธุรกิจ / การให้บริการที่มีความสำคัญ

The objectives of Business Continuity are fundamental

Viability	Keeping the company in business – strengthening the organization's ability to continue business in the face of disruption
People Protection	Protecting the company's employees and ensuring their well being
Earnings / Profit Protection	Protecting the company's financial commitments
Competitive Edge	Putting customers at ease by implementing business continuity programs and by developing business continuity capabilities
Brand Protection	Avoiding public embarrassment and loss of credibility

มุมมองของผู้บริหารต่อการพัฒนา BCM ในองค์กร

CEO / COO / CTO	• ลด หรือหลีกเลี่ยงการสูญเสียรายได้ • ปกป้องข้อมูลสำคัญ • ความปลอดภัยต่อชีวิตของพนักงานและลูกค้า • ปกป้องความเสียหายต่อทรัพย์สิน • ปกป้องภาพลักษณ์องค์กรและมูลค่าของผู้ถือหุ้น
Risk Manager	• เพื่อเสริมสร้างความตระหนักต่อภัยคุกคามและการควบคุมภายใน • เพื่อกระตุ้นให้เกิดการประสานงานระหว่างหน่วยงาน รวมถึงการสื่อสาร และการตัดสินใจในภาวะวิกฤต • เพื่อให้บรรลุความต้องการของลูกค้า และเป็นไปตามกฎ ระเบียบ ข้อบังคับต่างๆ ที่ต้องถือปฏิบัติ • เพื่อพัฒนาความสามารถในการตอบสนองต่อเหตุการณ์ฉุกเฉินได้อย่างมีประสิทธิภาพ • เพื่อเพิ่มขีดความสามารถในการเจรจาต่อรองสำหรับการจัดทำประกันความเสียหายของธุรกิจจากเหตุการณ์ภัยพิบัติ (Business Insurance)
Operation Manager	• เพิ่มความยืดหยุ่นในห่วงโซ่อุปทาน (Supply chain resilience) • เพื่อปกป้องกระบวนการทางธุรกิจที่สำคัญ • เพื่อให้สามารถกลับมาดำเนินงานได้เร็วที่สุดภายใต้ต้นทุนการดำเนินการที่เหมาะสม • เพื่อลดระดับผลกระทบและความเสียหายจากเหตุการณ์ให้น้อยที่สุด

บทเรียนจากการบริหารความต่อเนื่องทางธุรกิจที่พบได้บ่อยในปัจจุบัน

There is a gap in many organizations between management expectations and the company's ability to continue business operations.

Lessons Learned from Hundreds of Recoveries

1. Re-Evaluate longstanding assumptions in your **Risk Assessment**
2. Consider **Cascading Events** when you analyze your risk scenarios
3. Plan for risk scenarios with an **Extended Duration**
4. Prepare for the **Loss of Critical Infrastructure** — Especially Power
5. Validate the readiness of your **Critical Partners and Suppliers**
6. Remember that your **Employees are People First, Employees Second**
7. Develop **Robust Communication Strategies** using multiple modes
8. **Re-Evaluate your Site Strategy**
9. You must **Protect your Sensitive Data** — No matter what the circumstances

Source: *Deloitte's Cyber Risk Resilience*

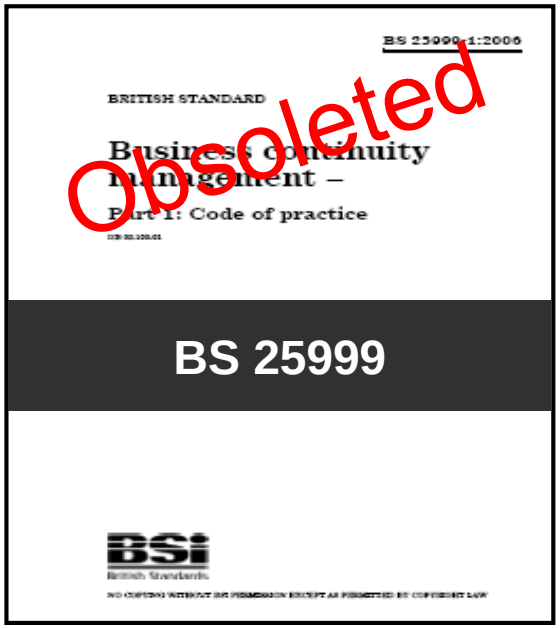
การบริหารความต่อเนื่องทางธุรกิจไม่ใช่แค่ปัญหาด้านเทคโนโลยี

2. แนวทางการพัฒนาระบบการบริหารความต่อเนื่องทางธุรกิจ

มาตรฐานสากลที่เกี่ยวข้อง

รหัส	ชื่อ	ปีที่เผยแพร่
ISO22300	Societal security – Terminology	2012
ISO22301	Societal security – Business continuity management systems - Requirements	2012
ISO22313	Societal security – Business continuity management systems - Guidance	2012
ISO22320	Societal security – Emergency management - Requirements for incident response	2011
มอก. 22301	มาตรฐานผลิตภัณฑ์อุตสาหกรรม – ระบบการบริหารความต่อเนื่องทางธุรกิจ – ข้อกำหนด	2553
ISO27001	Information Technology – Security techniques – information security management systems	2013

International Standard and Good Practices Guidelines

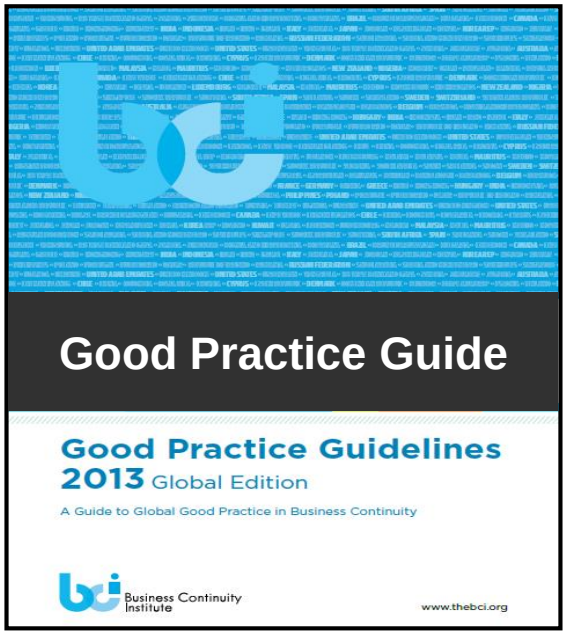


BS 25999

British National Standard for business continuity which establishes the process, principles and terminology of BCM.

ISO 22301

The new international BCM system standard released in May 2012



Good Practice Guide

Developed by Business Continuity Institute. Established in 1994, it is the leading institute for BCM professional membership and certification.

ISO 22301 Roadmap

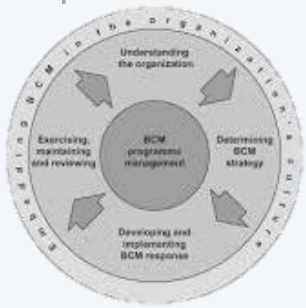
2006 2007 2008 2012 2013

BS25999-1:2006

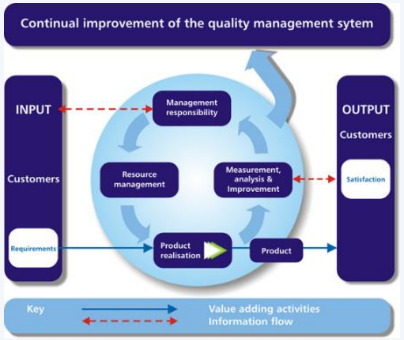
Code of Practice

BS25999-2:2007

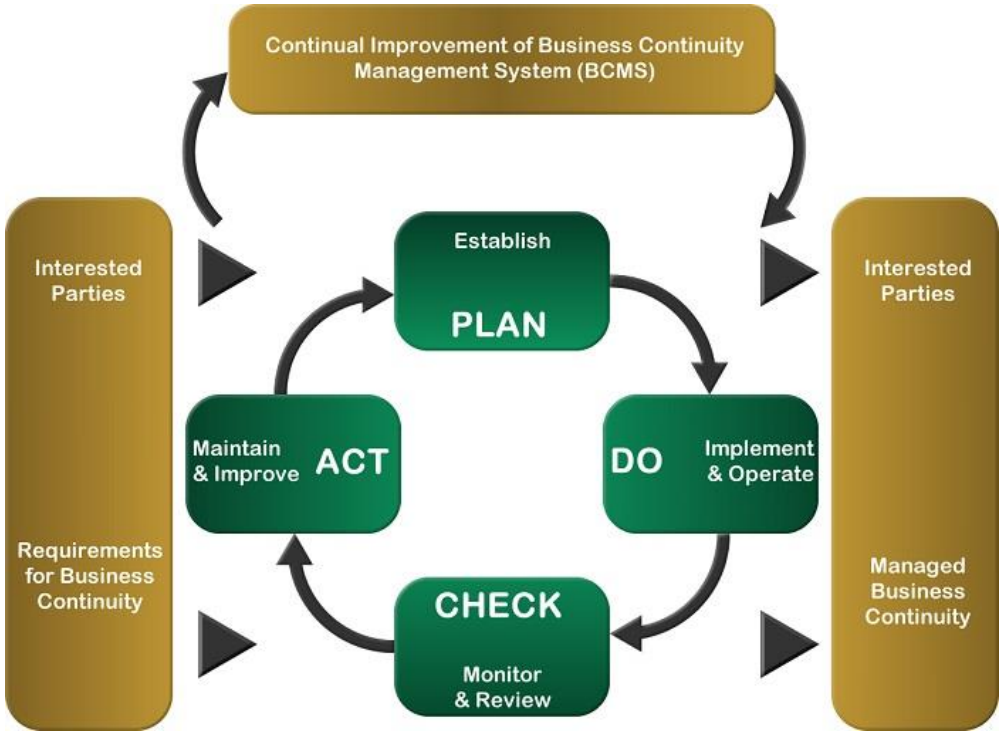
Specification



ISO 22301:2012



แนวทางการพัฒนาระบบการบริหารความต่อเนื่องทางธุรกิจ

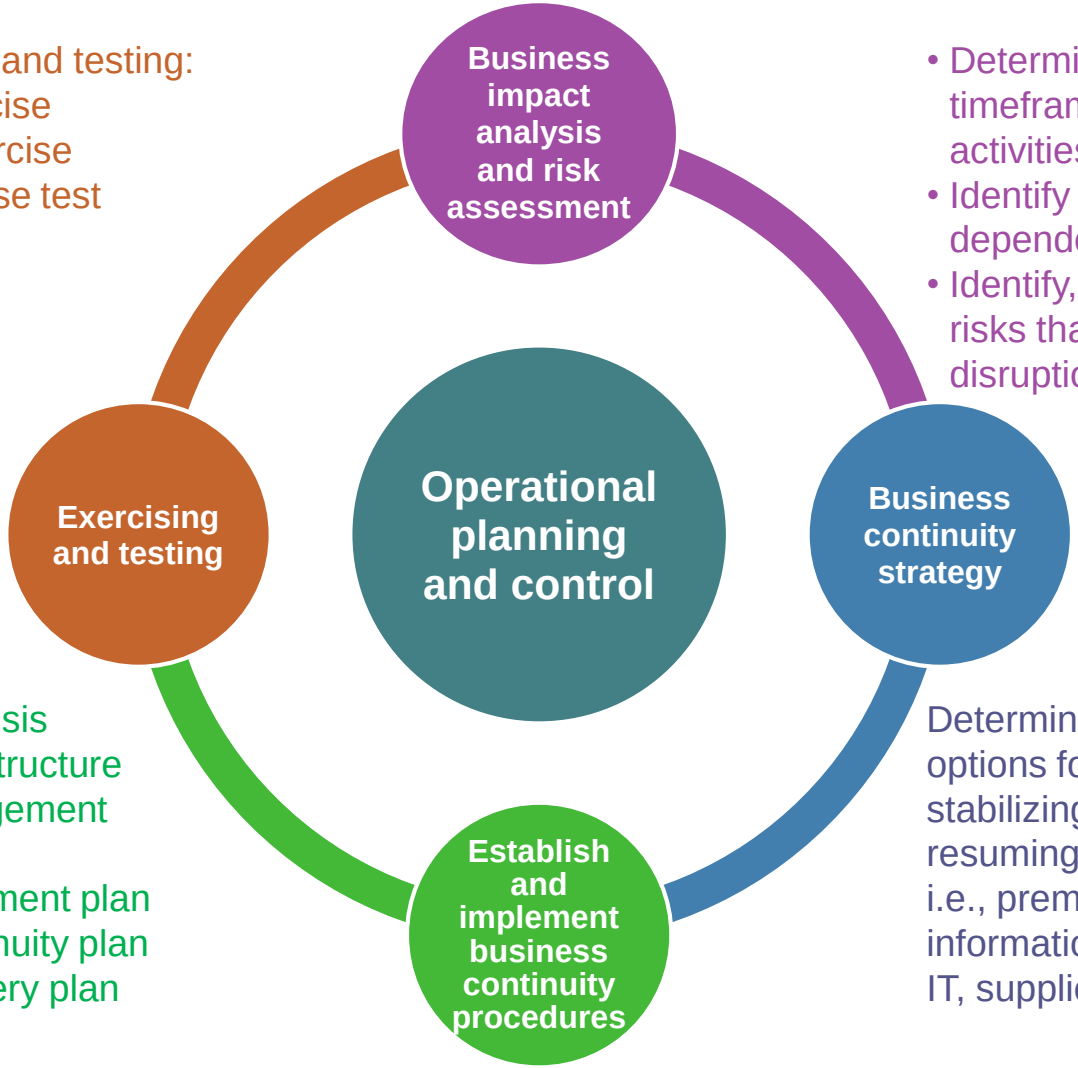


Plan (Establish)	Establish business continuity policy, objectives, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organization's overall policies and objectives.
Do (Implement and operate)	Implement and operate the business continuity policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against business continuity objectives and policy, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the BCMS by taking corrective actions, based on the results of management review and re-appraising the scope of the BCMS and business continuity policy and objectives.

Source: ISO22301: Business Continuity Management

องค์ประกอบของ BCM

Annual exercise and testing:
- Table-top exercise
- Simulation exercise
- Call tree surprise test



- Determine priorities and timeframes for resuming activities
- Identify the key resources and dependencies
- Identify, analyze and evaluate risks that could result in disruptions

- Incident and crisis management structure
- Incident management plan
- Crisis management plan
- Business continuity plan
- Disaster recovery plan

Determine appropriate strategy options for protecting, stabilizing, continuing, and resuming critical resources, i.e., premises, critical persons, information and vital records, IT, supplies.

Information security aspects of BCM

Information security continuity

- The organization shall determine its requirements for information security and the continuity of information security management in adverse situations
- The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
- The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

Redundancies

- Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements

Source: ISO/IEC27001:2013

องค์ประกอบของ BCM

- ความต้องการใช้ทรัพยากรในด้านต่างๆ
- การเตรียมความพร้อม

ทรัพยากรด้านต่าง ๆ

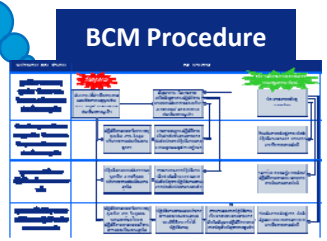
ผู้บริหารระดับสูง / คณะกรรมการ BCM

การเชื่อมโยงกับการบริหารความเสี่ยงองค์กร

Business Continuity Management

นโยบายการบริหารความต่อเนื่องทางธุรกิจ

กิจกรรมที่ต้องดำเนินการในสภาวะวิกฤต
ขั้นตอน ระยะเวลาดำเนินการ
ผู้ดำเนินการ ระดับการให้บริการ



กระบวนการ / กิจกรรม

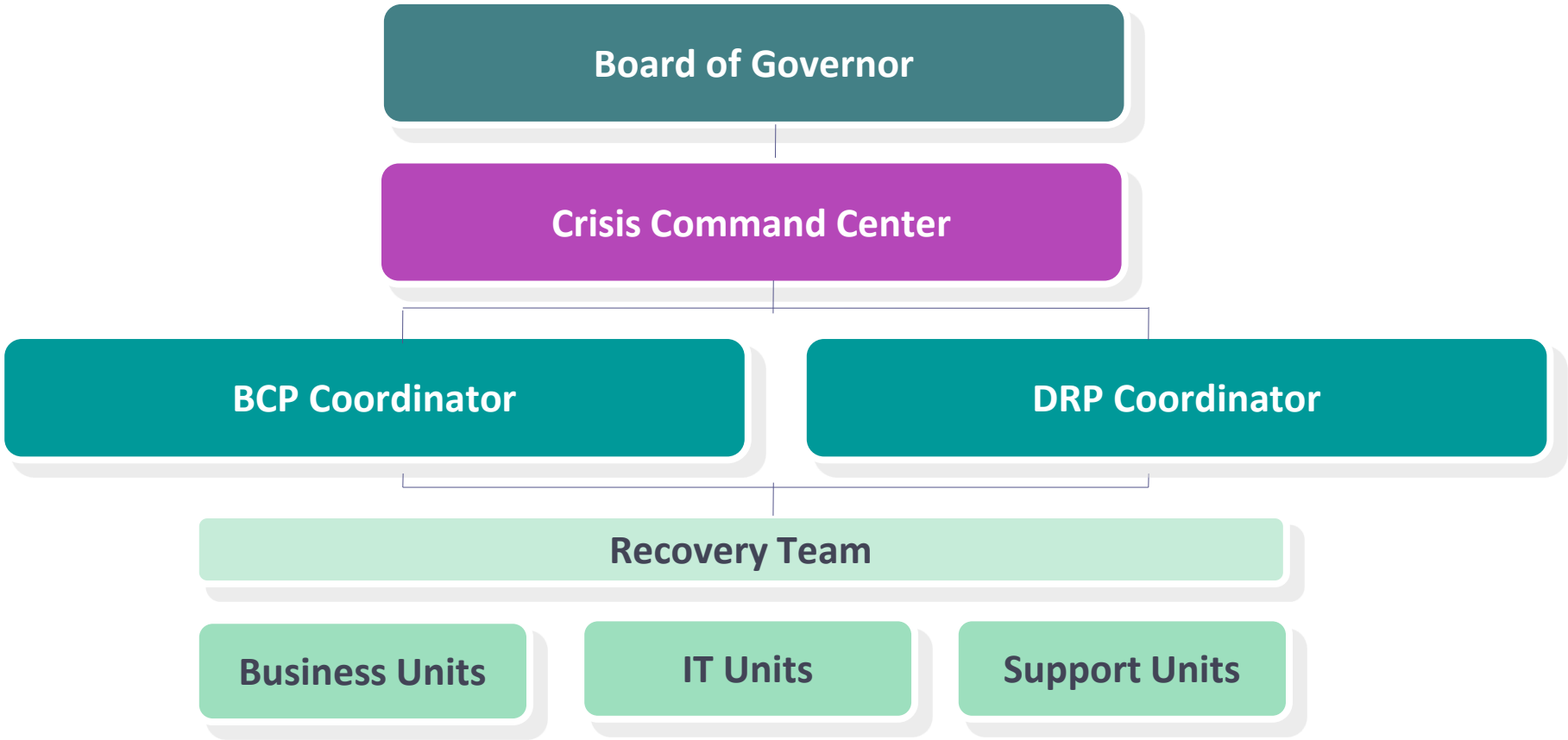
ผู้มีส่วนเกี่ยวข้อง

บทบาทและความรับผิดชอบ

การวางแผนระบบ BCM

- การกำหนดโครงสร้าง หน้าที่ และความรับผิดชอบของหน่วยงาน และบุคลากรที่เกี่ยวข้อง
- การเข้าใจบทบาท หน้าที่ และความรับผิดชอบในภาวะปกติ และภาวะวิกฤต
- การเข้าใจความสำคัญของงานบริการ และงานสนับสนุนที่เกี่ยวข้อง เพื่อกำหนดกระบวนการปฏิบัติงาน และ/หรือ งานบริการที่มีความสำคัญ

Establish a BCM Organization



ทำความเข้าใจองค์กร

ทำความเข้าใจองค์กร

(Understanding the organization)

- **การวิเคราะห์ผลกระทบต่อธุรกิจ**
- **การประเมินความเสี่ยง**
- **การกำหนดทางเลือก**

- อะไรคือ**<u>บริการหลักที่มีความสำคัญ</u>** ซึ่งหากเกิดการหยุดชะงักจากเหตุการณ์จะเกิดผลกระทบและความเสียหายเป็นอย่างมากต่อการดำเนินงานขององค์กร และจำเป็นต้องดำเนินการตามแผนเพื่อให้สามารถกลับมาดำเนินงาน / ให้บริการได้เร็วที่สุด
- กิจกรรม หรือ กระบวนการที่ใช้ในการดำเนินงานเพื่อให้องค์กรสามารถกลับมาดำเนินงาน / ให้บริการได้อย่างต่อเนื่อง
- อะไรคือ**<u>ทรัพยากรหลักที่จำเป็น</u>**ต้องใช้ในภาวะวิกฤต

สถานที่ปฏิบัติงาน

ระบบคอมพิวเตอร์

ข้อมูลสำคัญ

บุคลากรหลัก

อุปกรณ์และ
สิ่งอำนวยความสะดวก

ผู้มีส่วนได้สวนเสีย

การประเมินความเสี่ยงและผลกระทบทางธุรกิจ

แผนการป้องกันและบรรเทาสาธารณภัยแห่งชาติ พ.ศ. 2553-2557 แบ่งประเภทของภัยที่เกิดในประเทศไทยแบ่งออกเป็น 2 ประเภทหลัก รวมทั้งสิ้น 18 ภัย ดังนี้

(1) สาธารณภัยทั่วไป ประกอบด้วย 14 ภัย

(2) สาธารณภัยที่กระทบโดยตรงกับความมั่นคงของประเทศ ประกอบด้วย 4 ภัย

สาธารณภัยทั่วไป

1. อุทกภัย
2. ภัยจากพายุหมุนเขตร้อน
3. อัคคีภัย
4. ภัยจากสารเคมีและวัตถุอันตราย
5. ภัยจากการคมนาคมและขนส่ง
6. ภัยแล้ง
7. ภัยจากอากาศหนาว
8. ภัยจากไฟป่าและหมอกควัน
9. ภัยจากแผ่นดินไหวและอาคารถล่ม
10. ภัยจากคลื่นสึนามิ
11. ภัยจากโรคระบาดในมนุษย์
12. ภัยจากโรค แมลง สัตว์ ศัตรูพืช ระบาด
13. ภัยจากโรคระบาดสัตว์และสัตว์น้ำ
14. ภัยจากเทคโนโลยีสารสนเทศ

สาธารณภัยด้านความมั่นคง

1. ภัยจากการก่อวินาศกรรม
2. ภัยจากทุ่นระเบิด กับระเบิด
3. ภัยทางอากาศ
4. ภัยจากการชุมนุมประท้วงและก่อการจลาจล

ที่มา: *สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ*

ผลกระทบของภัยคุกคามต่อทรัพยากรที่มีความสำคัญ

อุทกภัย

สถานที่ปฏิบัติงาน

ระบบคอมพิวเตอร์

ข้อมูลสำคัญ

บุคลากรหลัก

อุปกรณ์และสิ่งอำนวยความสะดวก

ผู้มีส่วนได้สวนเสีย

ภัยจากเทคโนโลยีสารสนเทศ (Cyber Attack)

ระบบคอมพิวเตอร์

ข้อมูลสำคัญ

ผู้มีส่วนได้สวนเสีย

การบริหารความต่อเนื่องในการดำเนินงาน - ไฟไหม้สถานที่ทำการหลัก

ไฟไหม้

ผลกระทบ

อาคารที่ทำการเสียหาย

บุคลากรหลัก
ได้รับบาดเจ็บ

เครื่องแม่ข่ายเสียหาย

ข้อมูลและเอกสารสำคัญ
เสียหาย

อุปกรณ์และสิ่ง
อำนวยความสะดวก
เสียหาย

ผู้มีส่วนได้สวนเสียอื่นๆ

แนวทางการบริหารความต่อเนื่องในการดำเนินงาน

- ย้ายไปปฏิบัติงาน ณ สถานที่ปฏิบัติงานสำรอง
- ปฏิบัติงานจากที่บ้าน
- หยุดทำงานชั่วคราว

- สรรหาบุคลากรจากหน่วยงานอื่นมาปฏิบัติงานแทนชั่วคราว
- จ้างบุคลากรภายนอกมาปฏิบัติงานแทนชั่วคราว

- ใช้ระบบสารสนเทศ ณ ศูนย์คอมพิวเตอร์สำรอง
- ปฏิบัติงานมือ (Manual) ชั่วคราว

- ใช้สำเนาเอกสารที่มี
- ใช้ชุดข้อมูลสำรองที่จัดเก็บไว้

- จัดซื้ออุปกรณ์และสิ่งอำนวยความสะดวกมาใช้ทดแทน
- ยืมอุปกรณ์และสิ่งอำนวยความสะดวกจากหน่วยงานอื่น

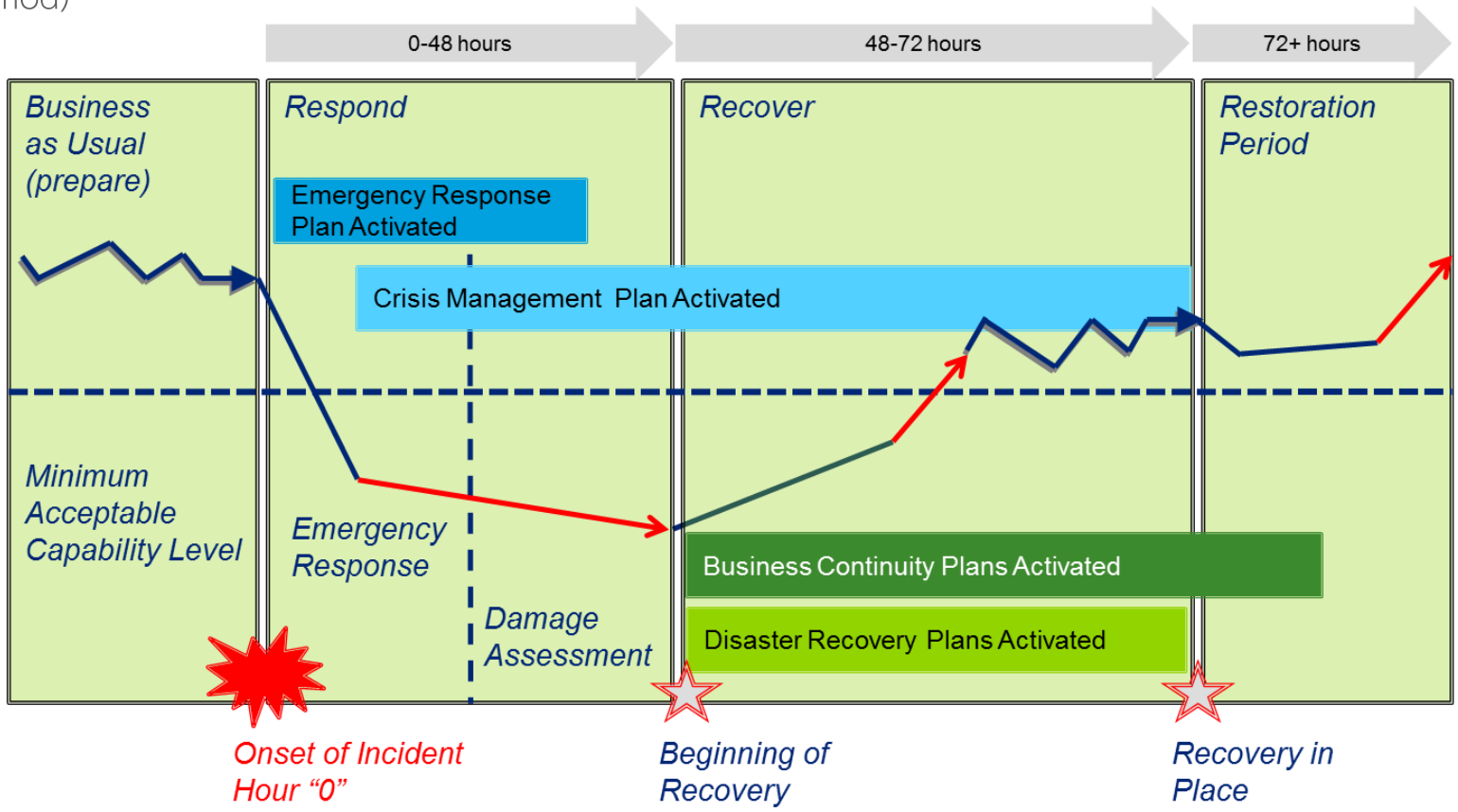
- ให้ประชาชนไปใช้บริการในพื้นที่ใกล้เคียง เช่น สาขาใกล้เคียง
- ใช้บริการจากผู้ขายรายอื่น

การบริหารความต่อเนื่องในการดำเนินงาน

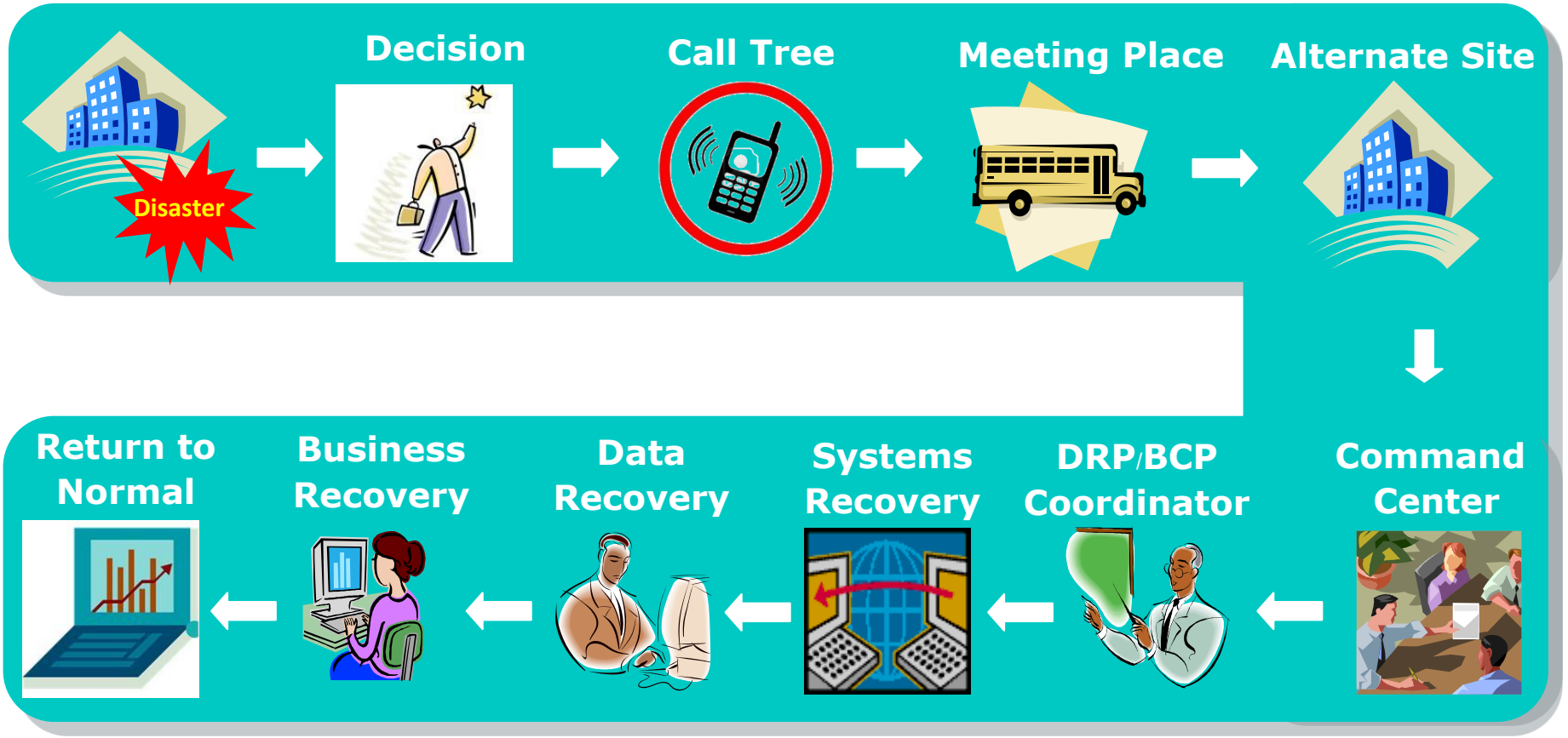
Area	Challenges/considerations
Building (Facilities)	• Identify critical facilities and implementing preparedness activities • Evaluating local risk levels, taking input from local civic authorities • Determining partial or complete facilities shutdowns • Waste disposal processes
Equipment	• Stabilizing the critical equipment environment and freeze changes (where applicable)
Technology	• Stabilizing the technology environment and freeze changes • Increasing remote working infrastructure (e.g., laptops, network bandwidth, remote access gateways, security tokens, voice and video conferencing) • Enabling and testing remote access to critical applications • Identifying critical technical support personnel
Human Resources	• Identifying critical roles and naming appropriate backups (possibly including contingent workers) • Distributing critical roles across geographies • Creating leadership succession plans and delegating decision making authority • Adjusting HR policies (e.g., travel, employees who fall ill, time-off, medical leaves, remote working, return to work, insurance) • Adding HR benefits (e.g., flu shots, antiviral medicines, medical support, employee assistance) • Consideration of international legal and cultural requirements • Identifying and supporting at-risk employees (e.g., primary caregivers to others, special needs) • Arranging for transportation for those who depend on public transit
3rd Parties	• Identifying key vendors, service providers, and suppliers • Confirming 3rd party preparedness and resilience • Identifying alternate sources as appropriate • Temporarily reducing SLAs and other requirements as appropriate • Establishing ongoing communications • Consideration of visitors, contractors, and consultants who work onsite at your organization

BCM Timeline

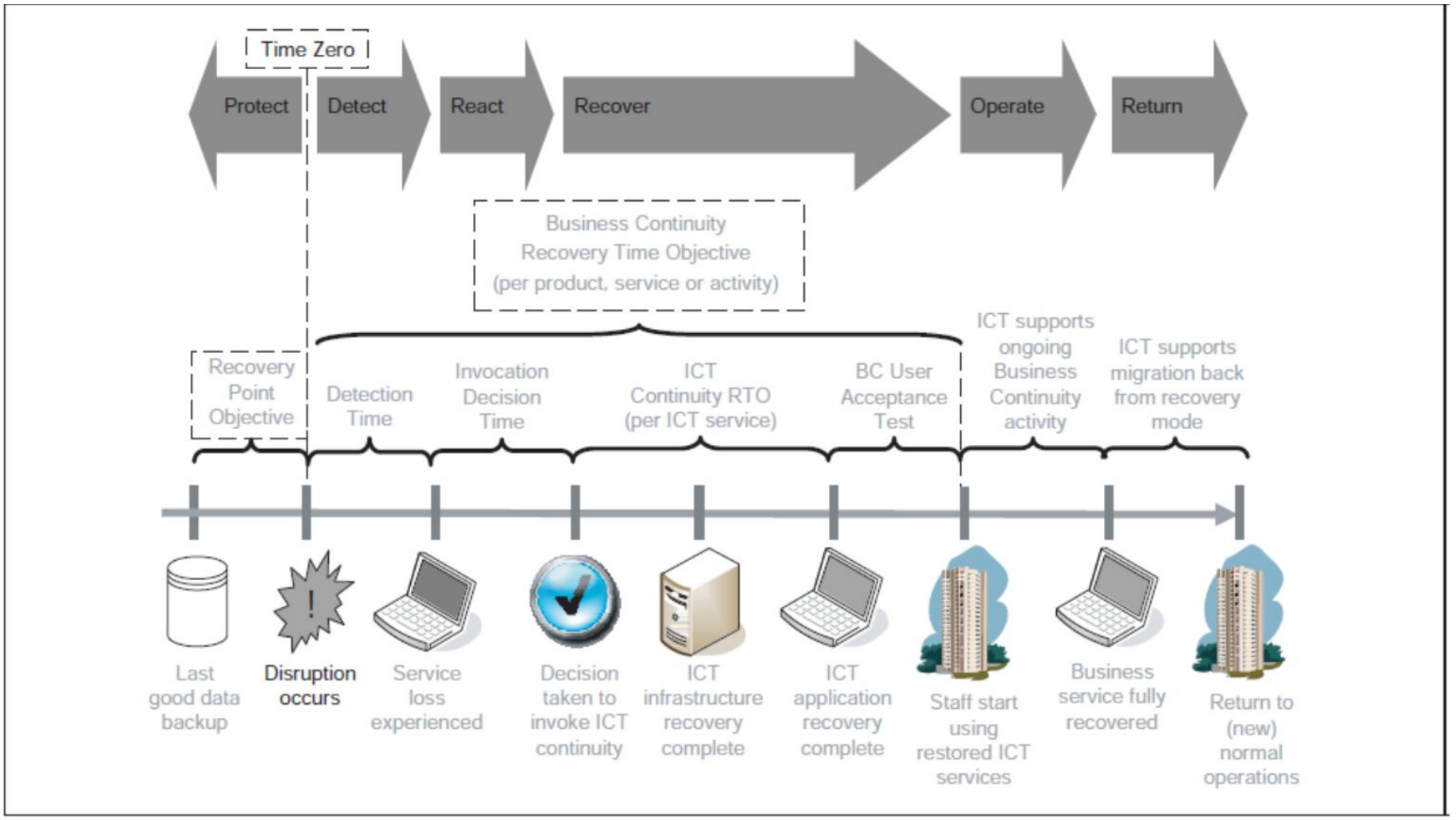
- การเผชิญเหตุ (Emergency responses) และการบริหารจัดการในภาวะวิกฤต (Crisis management) เริ่มต้นที่เวลา “0”
- มีการใช้แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plans) และแผนกู้ระบบ (IT Disaster Recovery Plan) ในช่วงระยะเวลาการฟื้นฟู (Recovery Period) จนกระทั่งสามารถกู้คืนกิจกรรม หรือกระบวนการทางธุรกิจที่สำคัญได้ (Restoration Period)



BCM Timeline



Key ICT continuity management timescales



Source: BS25777 ICT Continuity Management

การจัดทำแผน BCM และนำไปปฏิบัติ

การจัดทำแผน BCM และนำไปปฏิบัติ

(Developing and implementing BCM response)

โครงสร้างการตอบสนองต่ออุบัติการณ์

แผนการจัดการอุบัติการณ์และ
แผนความต่อเนื่องทางธุรกิจ

<u>แผนการจัดการอุบัติการณ์ (Incident Management Plan):</u>
แผนปฏิบัติการที่กำหนดไว้อย่างเป็นลายลักษณ์อักษร เพื่อใช้เมื่อเกิดอุบัติการณ์ โดยปกติจะครอบคลุมถึงบุคลากรหลัก ทรัพยากร การบริการ และการปฏิบัติการที่จำเป็นในการนำกระบวนการจัดการอุบัติการณ์ไปปฏิบัติ

<u>แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan):</u>
เอกสารที่รวบรวมขั้นตอนและข้อมูลซึ่งทำให้องค์กรพร้อมที่จะนำไปใช้เมื่อเกิดอุบัติการณ์ เพื่อให้สามารถดำเนินการในกิจกรรม หรือกระบวนการหลักในระดับที่กำหนดไว้

ที่มา: มอก. 22301-2553

การฝึกซ้อม การรักษา และการทบทวนการจัดเตรียมการเกี่ยวกับ BCM

การฝึกซ้อม การรักษา และการทบทวนการจัดเตรียมการเกี่ยวกับ BCM

(Exercising, maintaining and reviewing)

ดำเนินการฝึกซ้อม ทบทวน และทำให้เป็นปัจจุบัน

การรักษาและทบทวนการเตรียมการเกี่ยวกับ BCM

ฝึกซ้อมแผนเผชิญเหตุและแผนความต่อเนื่องทางธุรกิจตามสถานการณ์ที่กำหนด

ทบทวน และทำให้เป็นปัจจุบันอย่างสม่ำเสมอ

- เพื่อให้มั่นใจว่าระบบ BCM ที่จัดเตรียมไว้สามารถนำไปปฏิบัติได้อย่างมีประสิทธิผลตามที่ต้องการ
- เพื่อประเมินความถูกต้องและครบถ้วนของข้อมูลในแผนความต่อเนื่องทางธุรกิจ
- เพื่อให้มั่นใจว่าหน่วยงานสามารถตอบสนองต่อสถานการณ์ที่เกิดขึ้น ตลอดจนกอบกู้ทรัพยากรและกระบวนการทำงานต่างๆ และกลับสู่ภาวะการดำเนินธุรกิจตามปกติได้ภายในระยะเวลาและเงื่อนไขที่กำหนด
- เพื่อทดสอบและยืนยันสิ่งที่ได้มีการเตรียมการไว้สามารถทำให้ธุรกิจสามารถดำเนินการได้อย่างต่อเนื่อง
- เพื่อนำผลลัพธ์ที่ได้จากการทดสอบไปปรับปรุงแผนความต่อเนื่องทางธุรกิจให้มีความสมบูรณ์มากยิ่งขึ้น

ปัจจัยความสำเร็จของการบริหารความต่อเนื่องทางธุรกิจขององค์กร

- การมีส่วนร่วมหรือการให้คำมั่นสัญญาของผู้บริหาร
- ความร่วมมือของพนักงานที่เกี่ยวข้อง
- การกำหนดขอบเขตและความต้องการที่ชัดเจน
- การสื่อสารที่มีประสิทธิผล
- การกำหนดความเป็นเจ้าของแผน
- การพัฒนาวัฒนธรรมองค์กรเกี่ยวกับความตระหนักของการบริหารความต่อเนื่องทางธุรกิจภายในองค์กร

3. กรณีศึกษาเรื่องการบริหารความต่อเนื่องทางธุรกิจ

March 2011: The Great Tsunami hit Japan

การเตรียมตัวของญี่ปุ่นกับแผ่นดินไหวและสึนามิ

"…Japan, of all countries in the world, is probably most prepared for what happened…"

Berman, the Executive Director of DRI International

".."Because earthquakes are commonplace in Japan, earthquake drills are a normal part of life and the population lives with an ongoing awareness that the potential for disaster always looms"…

Linda Lowen, national awards broadcast journalist

กลไกการบริหารจัดการ

รัฐบาลญี่ปุ่นได้มีการออกกฎหมายและปรับปรุงกฎหมายเพื่อยกระดับมาตรฐานการเตรียมพร้อม ป้องกัน และรับมือกับภัยพิบัติ ได้แก่

(1) กฎหมายที่เกี่ยวกับภัยพิบัติ

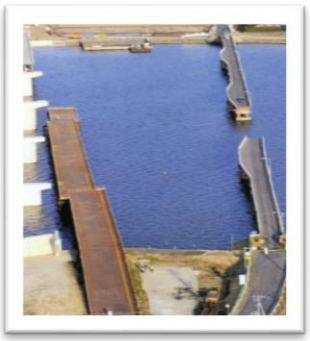
(2) กฎหมายที่เกี่ยวกับแผ่นดินไหว

(3) กฎหมายเพื่อป้องกันอุบัติภัยจากนิวเคลียร์

รัฐบาลญี่ปุ่นยังมีแผนประสานงานภายหลังการเกิดภัย โดยส่งเสริมให้ภาคเอกชน องค์กรต่างๆ และประชาชนทั่วไปเผชิญภัยพิบัติด้วยหลักความรับผิดชอบ สามารถพึ่งตนเองและช่วยเหลือกันอย่างมีประสิทธิภาพ

ผลกระทบจากเหตุการณ์

- ธนาคารโลกได้ประมาณความเสียหายไว้ประมาณ 235,000 ล้านเหรียญสหรัฐ ถือเป็นมูลค่าความเสียหายจากภัยธรรมชาติที่สูงที่สุดในโลก โดยความเสียหายนี้ไม่รวมความเสียหายที่อาจเกิดจากผลกระทบจากการรั่วไหลของสารกัมมันตรังสีจากโรงไฟฟ้านิวเคลียร์ฟูกูชิมะ
- โครงสร้างพื้นฐานเสียหาย เช่น สนามบิน โรงไฟฟ้า ถนน ท่าเรือ สะพาน เรือขนส่ง รถไฟ เป็นต้น
- ผู้เสียชีวิต 15,373 คน ผู้ได้รับบาดเจ็บ 5,364 คน และอีก 8,198 คนยังคงหายสาบสูญ ใน 18 จังหวัด
- บ้านเรือนราว 4.4 ล้านหลังคาเรือนทางตะวันออกเฉียงเหนือของญี่ปุ่นไม่มีกระแสไฟฟ้าใช้ และ อีก 1.5 ล้านคนไม่มีน้ำใช้
- ประชาชนไร้ที่อยู่อาศัย จำนวนอาคารบ้านเรือนที่เสียหายมีทั้งสิ้นอย่างน้อย 111,044 หลัง และการเสียขวัญกำลังใจของประชาชน ที่ไม่สามารถประเมินได้




สิ่งที่ตามมาภายหลังสึนามิ

การขนส่งและ
โทรคมนาคม

ระบบผลิตและจำหน่าย
ไฟฟ้า

ผลกระทบต่อธุรกิจ
ในภาคต่าง ๆ

อุตสาหกรรม / การลงทุน

ผลกระทบด้านขนส่ง

ผลกระทบ

- ท่าเรือทั้งหมดของญี่ปุ่นปิดชั่วคราวหลังจากเกิดแผ่นดินไหว มีท่าเรือจำนวน 4 ท่าถูกทำลาย และอีก 10 ท่าได้รับความเสียหาย ซึ่งคาดว่าต้องใช้เวลาหลายสัปดาห์กว่าจะกลับมาให้บริการได้
- รถไฟหัวกระสุนสายโทโฮะกุหลายส่วนที่อยู่ทางตอนเหนือของญี่ปุ่นได้รับความเสียหายบริการรถรางหยุดชะงักในโตเกียว
- ท่าอากาศยานเซนไดน้ำท่วม ท่าอากาศยานนานาชาตินาริตะและฮาเนดะได้ชะลอการให้บริการหลังจากแผ่นดินไหว
- บริการรถไฟทั่วญี่ปุ่นจำนวนมากถูกยกเลิก

มาตรการบริหารความต่อเนื่อง

- รถไฟหัวกระสุนสายโทไดโดชินกันเซ็นได้กลับมาให้บริการอีกครั้ง แต่ไม่ทั้งหมด ภายในวันเดียวกัน และเปิดให้บริการตามตารางเวลาปกติภายในวันรุ่งขึ้น ในขณะที่สายโจเอ็ตสุและนางาโนะชินกันเซ็นได้กลับมาให้บริการอีกครั้งในวันรุ่งขึ้น สายโทโฮะกุกลับมาให้บริการอีกครั้งเมื่อวันที่ 15 มีนาคม โดยมีการให้บริการไปอย่างเดียวหนึ่งขบวนต่อชั่วโมงระหว่างโตเกียวและนาสุ-ชิโอบาระ
- เที่ยวบินส่วนใหญ่เปลี่ยนไปลงท่าอากาศยานแห่งอื่นเป็นเวลาราว 24 ชั่วโมง
- สายการบินสิบสายที่ปฏิบัติการที่นาริตะได้ย้ายที่ทำการยังฐานทัพอากาศโยโกตะที่อยู่ใกล้เคียงแทน

เครือข่ายการขนส่งของญี่ปุ่นหยุดชะงักอย่างรุนแรง

ผลกระทบด้านโทรคมนาคม

ผลกระทบ

- บริการโทรศัพท์เคลื่อนที่และสายดินได้รับผลกระทบอย่างมากในพื้นที่แผ่นดินไหว
- บริการอินเทอร์เน็ตส่วนใหญ่ไม่ได้รับผลกระทบในพื้นที่ที่สาธารณูปโภคพื้นฐานยังคงมีอยู่
- ระบบเคเบิลใต้ทะเลหลายส่วนในพื้นที่ที่ได้รับความเสียหายจากแผ่นดินไหวแต่ไม่สร้างผลกระทบมากนัก เนื่องจากระบบเหล่านี้มีการรองรับในส่วนสายเคเบิล redundant และมีการ loop เชื่อมต่อกันเป็นใยแมงมุมในญี่ปุ่น
- มีเพียงไม่กี่เว็บไซต์เท่านั้นที่ไม่สามารถเข้าถึงได้

มาตรการบริหารความต่อเนื่อง

- ผู้ให้บริการ Hot Spot WiFi หลายแห่งได้รับมือกับเหตุแผ่นดินไหวโดยให้บริการเข้าถึงเครือข่ายของพวกเขาฟรี
- ญี่ปุ่นใช้ “3G” ในการติดต่อสื่อสาร การสื่อสารทางอินเทอร์เน็ตจึงไม่ค่อยได้รับผลกระทบ สังเกตได้จากคนไทยยังสามารถติดต่อเพื่อนผ่านทาง Facebook ณ เวลาเกิดเหตุ

หากเหตุการณ์เกิดขึ้นกับประเทศไทย การติดต่อสื่อสารช่องทางใดยังสามารถใช้การได้ ???

ผลกระทบด้านระบบผลิตและจำหน่ายไฟฟ้า

ผลกระทบ

- เตาปฏิกรณ์โรงไฟฟ้านิวเคลียร์ทั้งหมด 55 เตา หยุดกำลังการผลิตไป 11 เตา
- ส่งผลให้กระแสไฟฟ้าจากโรงไฟฟ้านิวเคลียร์หายไป 25% หรือคิดเป็น 8% ของไฟฟ้าทั้งหมด
- TEPCO ไม่สามารถผลิตกระแสไฟฟ้าได้เนื่องจากเตาปฏิกรณ์ได้รับความเสียหาย KEPCO ไม่สามารถสามารถแบ่งกระแสไฟฟ้าให้ได้ เนื่องจากระบบของบริษัททำงานอยู่ที่ 60Hz ขณะที่ TEPCO ทำงานที่ 50Hz

มาตรการบริหารความต่อเนื่อง

- สลับกันตัดไฟฟ้าในเมืองต่างๆ ใน 8 จังหวัดภาคกลาง โดยแบ่งเป็นกลุ่ม กลุ่มละ 4 ชั่วโมง

ปัจจุบันญี่ปุ่นไม่มีสายส่งไฟฟ้าแห่งชาติ ดังนั้นการโอนถ่ายกระแสไฟฟ้าในญี่ปุ่นจึงทำได้ยาก

ผลกระทบด้านอุตสาหกรรม / การลงทุน

ผลกระทบ

- บริษัทอุตสาหกรรมการผลิตรถยนต์หยุดการผลิตอัตโนมัติ
- บริษัทในอุตสาหกรรมอิเล็กทรอนิกส์บางส่วนชะลอการผลิตที่โรงงานอุตสาหกรรมทั้งหมดหกแห่งในพื้นที่ ขณะที่บางส่วนไม่สามารถดำเนินการผลิตต่อได้ในโรงงานอุตสาหกรรมเกือบทั้งหมดในจังหวัดกุนมะและจังหวัดโทะชิงิ

มาตรการบริหารความต่อเนื่อง

- บริษัทรถยนต์และอุตสาหกรรมในพื้นที่ที่ได้รับผลกระทบหยุดการผลิต และลดกำลังการผลิต
- ให้พนักงานสับเปลี่ยนกันหยุดงาน เพื่อลดต้นทุนการผลิต
- เจรจากับลูกค้าในการเลื่อนการส่งสินค้า
- จัดหาผู้ผลิตชิ้นส่วนหรืออะไหล่ทดแทน
- เพิ่มกำลังการผลิต


คนญี่ปุ่นกับการรับของตอนเกิดสึนามิ

Nov 2008: India's perspective on terrorism

In 2008, a series of shooting and bombing attacks in the Indian city of Mumbai lasted for four days and resulted in the deaths of 164 people.

Terrorism is not unheard of in India but the scale of this attack was previously unimaginable, so much so that it is now often described as India's 9/11.

The physical damage caused by such events do not take long to recover from but the fear factor that they bring usually lasts for much longer. The reputational damage and the economic damage do take time to recover from.

Feb 2011: Earthquakes in Christchurch

Christchurch at 12.51pm on Tuesday 22 February 2011,

Inland Revenue had just one central office of over 800 staff members in the center of town.

"In response, available senior managers met and began the work of assigning new roles and tasks to staff. One of their immediate challenges was making contact with their people to ensure that they were all safe."

Some of the best laid emergency plans simply won't work in a real life situation, so *a flexible workforce is essential.*

Prior to the earthquake, Inland Revenue had no formal program of flexible work, so everything had to be developed immediately.

Challenges

- How to manage and monitor people from a distance?
- What kinds of tasks could be done at home?
- What policies and processes need to be announced in that period?

2013: Interruption to utility supply

One of the most high profile interruptions to utility supply during 2013 took place at the Superbowl, as early on in the third quarter, the stadium was cast into darkness.

"The Superbowl is the climax to the NFL season and is watched by over 100 million people in the US, in addition to the viewers in 80 other countries across the world who all screen it live.

The power was out for only 22 minutes and the game was delayed for a total of 34 minutes – not long but exceptionally significant."

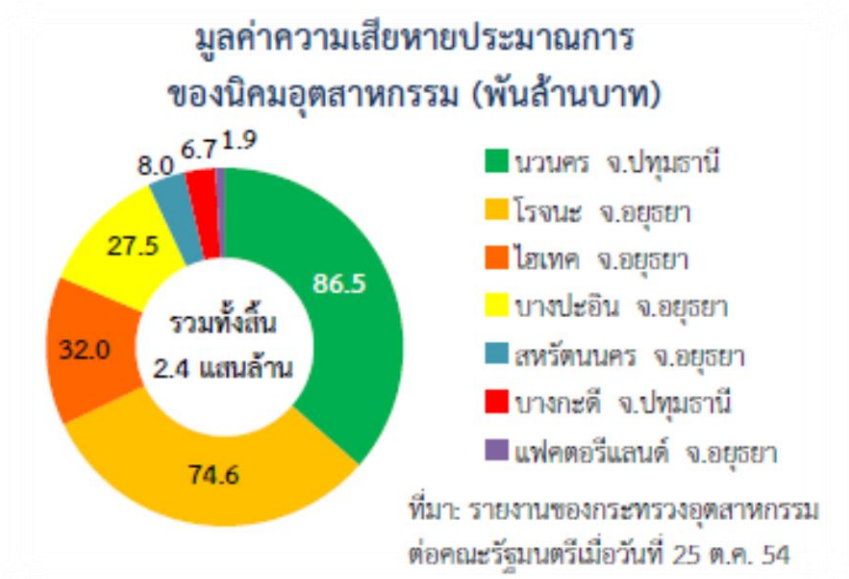
The Superbowl is a big money event with advertisers paying $4million for a 30 second commercial….

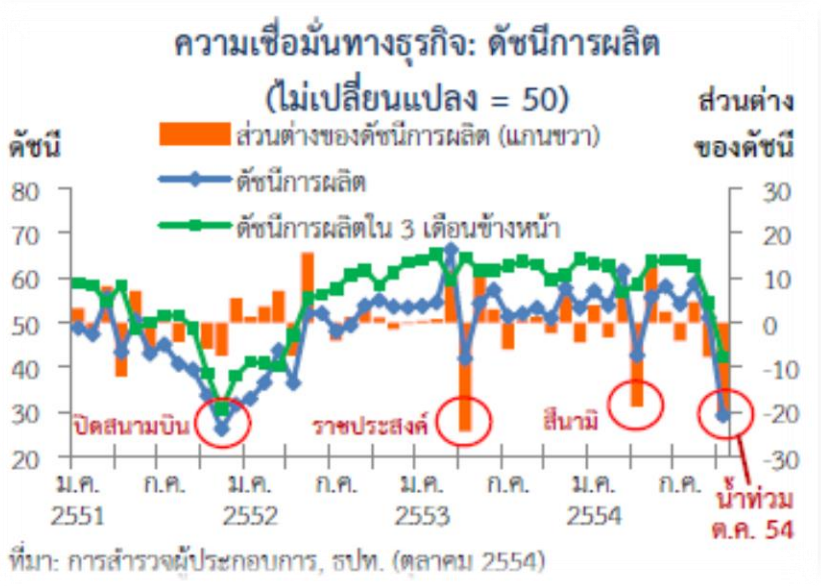
With no action on the field however, viewers soon start to switch off. If the advertisers felt like they lost out and did not get value for money, they may be reluctant to return next time….

Source: *Horizon Scan 2014 Survey Report, BSI*

- What would the cost be to your organization, direct or indirect, if power went out either for a short period of time or for longer?
- If a power failure can occur at one of the most high profile events in the world, at a venue that had undergone significant investment to prevent such an incident, what are the chances of it happening at your organization?
- If your organization was unable to deliver the service you had been contracted to do, would you open yourselves up to legal action?

มหาอุทกภัย 2554





- เหตุการณ์เริ่มขึ้นตั้งแต่วันที่ 25 กรกฎาคม 2554 ในพื้นที่ภาคเหนือ และแผ่ขยายวงกว้างครอบคลุมพื้นที่ภาคกลางและภาคตะวันออกเฉียงเหนือรวมทั้งสิ้น 64 จังหวัด โดยสถานการณ์ได้รุนแรงขึ้นตามลาดับจนเข้าสู่จุดสูงสุดในเดือนตุลาคม
- เหตุการณ์น้าท่วมนิคมอุตสาหกรรมครั้งแรกในประวัติศาสตร์จำนวน 7 แห่งในจังหวัดอยุธยาและปทุมธานี
- ในเบื้องต้นประเมินว่าความเสียหายของโรงงานในนิคมอุตสาหกรรมจะอยู่ที่ 2.4 แสนล้านบาท และโรงงานนอกนิคมอุตสาหกรรมอยู่ที่ 2.4 แสนล้านบาท
- พื้นที่การเกษตรได้รับความเสียหายประมาณ 11.4 ล้านไร่
- ธปท. ประเมินว่าเศรษฐกิจไทยในไตรมาสที่ 4 จะหดตัวลงมาก และทั้งปี 2554 เศรษฐกิจขยายตัวลดลงจากร้อยละ 2.6 เหลือเพียงร้อยละ 1.8 (ประมาณการ 30/11/2554)

Source: Bank of Thailand

ผลกระทบและแนวโน้มการฟื้นตัวของธุรกิจในประเทศ

ธุรกิจอสังหาริมทรัพย์

- ความต้องการในตลาดอสังหาริมทรัพย์หยุดชะงักลง
- ผู้ประกอบการคาดว่าตลาดอสังหาริมทรัพย์จะใช้เวลาฟื้นตัวประมาณ 6 เดือนเพื่อกลับสู่สภาวะปกติ
- ผู้ประกอบการคาดว่าผู้บริโภคจะย้ายทำเลหนีพื้นที่น้ำท่วม และย้ายประเภทบ้านจากแนวราบไปอยู่อาคารชุดเพิ่มขึ้น แต่ไม่สูงมากอย่างมีนัยสาคัญ เนื่องจากปัจจัยสาคัญในการซื้อที่อยู่อาศัยยังคงเป็นทำเลที่ตั้ง ซึ่งใกล้กับสถานที่ทางาน

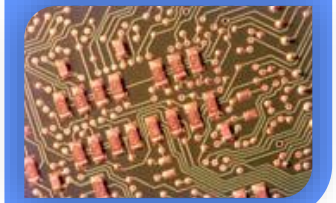
อุตสาหกรรมยานยนต์และชิ้นส่วน

- อุทกภัยส่งผลกระทบอย่างมากต่อบริษัทประกอบรถยนต์และบริษัทผู้ผลิตชิ้นส่วนยานยนต์
- ลดปริมาณการผลิตลง หรือ หยุดการผลิตชั่วคราว เพื่อหาวัตถุดิบจากแหล่งใหม่ ส่งผลให้การผลิตรถยนต์ในปี 2554 ลดลงประมาณ 3-3.5 แสนคัน เทียบกับเหตุการณ์สึนามิญี่ปุ่น ซึ่งทาให้การผลิตรถยนต์ของไทยลดลงไปราว 1 แสนคัน
- ในปี 2555 ผู้ประกอบการยังคงเป้าหมายการผลิตรถยนต์ที่ 2 ล้านคันต่อปี โดยมีแผนเร่งการผลิตอย่างเต็มที่

อุตสาหกรรมเครื่องใช้ไฟฟ้า

- ได้รับผลกระทบจากอุทกภัยในสัดส่วนที่น้อยกว่าอุตสาหกรรมอิเล็กทรอนิกส์ ส่วนหนึ่งเพราะเครื่องใช้ไฟฟ้ามีผู้ผลิตหลายรายและกระจายอยู่ในหลายพื้นที่
- ผู้ประกอบการบางรายได้ลงทุนสร้างพนังป้องกันน้ำท่วมโรงงาน ย้ายสินค้าและวัตถุดิบไปไว้ในที่ปลอดภัย ย้ายเครื่องจักรไปผลิตที่โรงงานอื่นซึ่งน้ำไม่ท่วม เพิ่มการผลิตที่โรงงานต่างประเทศทดแทน
- ผู้ประกอบการส่วนใหญ่ยังลงทุนตามแผนเดิม แต่อาจมีการเลื่อนแผนลงทุนออกไปบ้างเพื่อฟื้นฟูโรงงานก่อน

อุตสาหกรรมอิเล็กทรอนิกส์



- ได้รับผลกระทบมากเนื่องจากโรงงานส่วนใหญ่กระจุกตัวในบริเวณที่ได้รับความเสียหายจากน้าท่วมโดยตรง
- ผู้ผลิต Hard Disk Drive (HDD) รายใหญ่และ Supplier จำนวนมากในอยุธยาและปทุมธานีถูกน้ำท่วมจนต้องหยุดผลิตชั่วคราว ส่งผลให้ผู้ผลิต HDD รายอื่นนอกพื้นที่ต้องชะลอการผลิตลงเนื่องจากขาดแคลนวัตถุดิบ รวมถึง ปรับขบวนการผลิตให้สอดคล้องกับวัตถุดิบที่มีอยู่ การให้ Supplier ย้ายไปผลิตที่โรงงานอื่น การหา Supplier รายใหม่จากในประเทศ การนำเข้าชิ้นส่วนจากต่างประเทศเพิ่มขึ้น การย้ายแรงงานและเครื่องจักรไปผลิตที่โรงงานอื่นในต่างจังหวัด เพิ่มการผลิตในโรงงานต่างประเทศเพื่อชดเชยโรงงานที่ถูกน้ำท่วม
- ในอนาคตผู้ผลิตจะกระจายความเสี่ยงโดยลงทุนในภูมิภาค หรือในต่างประเทศมากขึ้น

การฟื้นฟูธุรกิจของภาคเอกชนได้ทยอยดำเนินการและจะใช้เวลาประมาณครึ่งปีที่จะกลับเข้าสู่ภาวะปกติ สะท้อนถึงความยืดหยุ่นในการปรับตัวและความทนทานของธุรกิจไทย การฟื้นตัวดังกล่าวจะช่วยสร้างความเชื่อมั่นของประชาชนให้กลับคืนมา และเอื้อต่อการขยายตัวของเศรษฐกิจในปี 2555

Source: Bank of Thailand

4. ผลสำรวจด้านการบริหารความต่อเนื่องทางธุรกิจ

Top threats in 2014

The top three threats rated by level of concern in this year's survey are:

- **Unplanned IT and telecom outages**
  (77% extremely concerned or concerned)
- **Data breach**
  (73% extremely concerned or concerned)
- **Cyber attack**
  (73% extremely concerned or concerned)

"It is clear from this that the threat to information systems is considered much more of an issue than the threat to anything else."

Source : *Horizon Scan 2014 Survey Report, BSI*

"Both Japan and New Zealand have suffered as a result of natural disasters in recent years and this was evident in the survey with respondents from both countries rating earthquake/tsunamis higher than any digital threat."

Cyber Security Incidents

48% risen in a world, 42.8 Millions time, *117,339* attacks per day

Average financial loss from cybersecurity incidents was $2.7 million

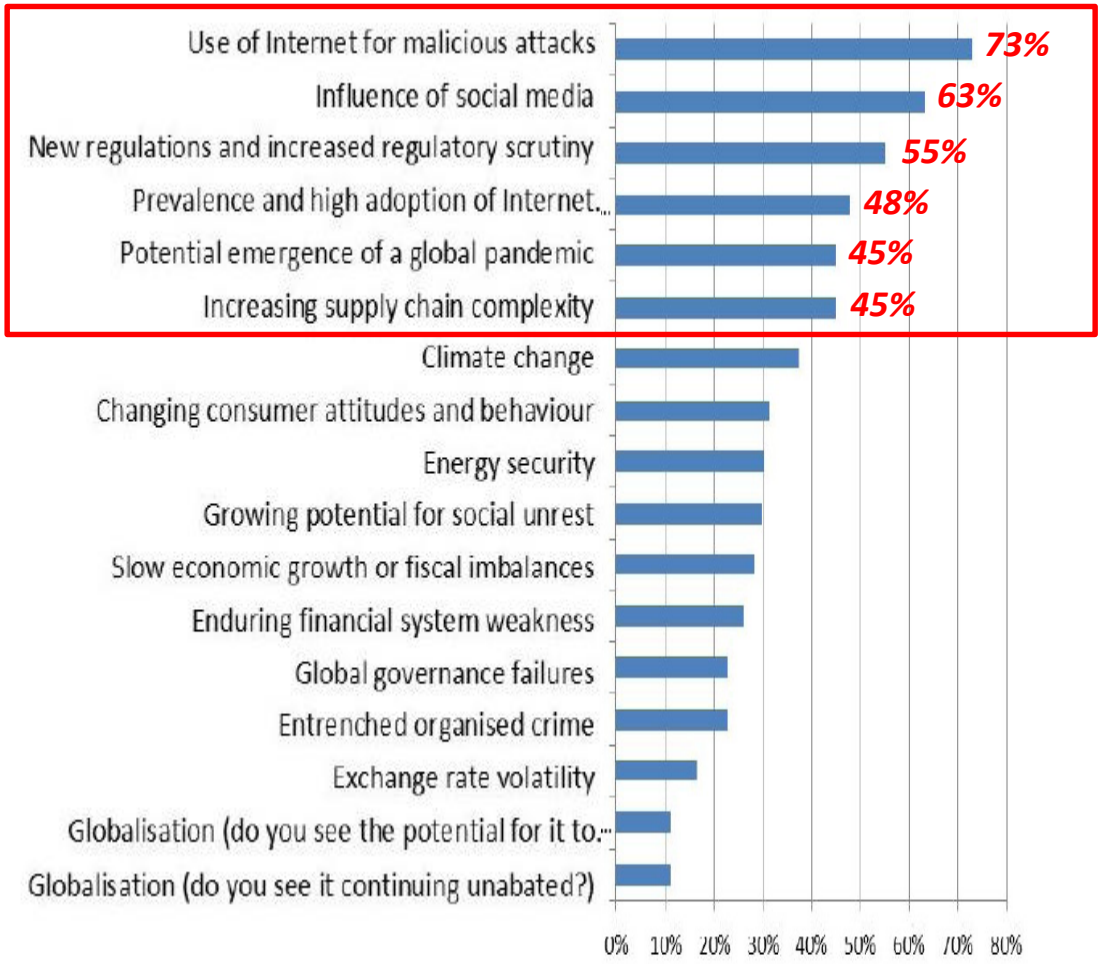
– a *34%* increase over 2013, Security spending as a percentage of IT

budget has remained stalled at *4%* ⬇

Source: *Global State of Information Security Survey 2015*

Top trends

The survey asked whether any of the 17 identified trends, emerging trends or uncertainties were on the respondent's radar for evaluation in terms of their business continuity implications.



Top 5... for business

[1] Internet for malicious attacks

[2] Influence of social media

[3] New reg. & increase regulatory

[4] Prevalence & high adoption of Internet

[5] Global pandemic

[5] Increasing supply chain complexity

Source : *Horizon Scan 2014 Survey Report, BSI*

Top 3 threats and trends

Comparison by geographic location of the organization.

	Asia	Europe	USA	NZ	JP
No. of respondents	74	227	93	14	23
Top 3 threats	1. Data breach 2. Unplanned IT or telecom outages 3. Human illness	1. Unplanned IT or telecom outages 2. Cyber attack 3. Data breach	1. Cyber attack 2. Unplanned IT or telecom outages 3. Data breach	1. Earthquake/ tsunami 2. Cyber attack 3. Adverse weather 3. Interruption to utility supply	1. Earthquake/ tsunami 2. Data breach 3. Human illness
Top 3 trends	1. Use of the internet for malicious attacks 2. Influence of social media 3. Potential emergence of a global pandemic	1. Use of the internet for malicious attacks 2. Influence of social media 3. New regulations and increased regulatory scrutiny	1. Use of the internet for malicious attacks 2. New regulations and increased regulatory scrutiny 3. Influence of social media	1. Influence of social media 2. Use of the internet for malicious attacks 3. High adoption of internet dependent services	1. Potential emergence of a global pandemic 2. Climate change Increasing supply chain complexity 3. Use of the internet for malicious attacks

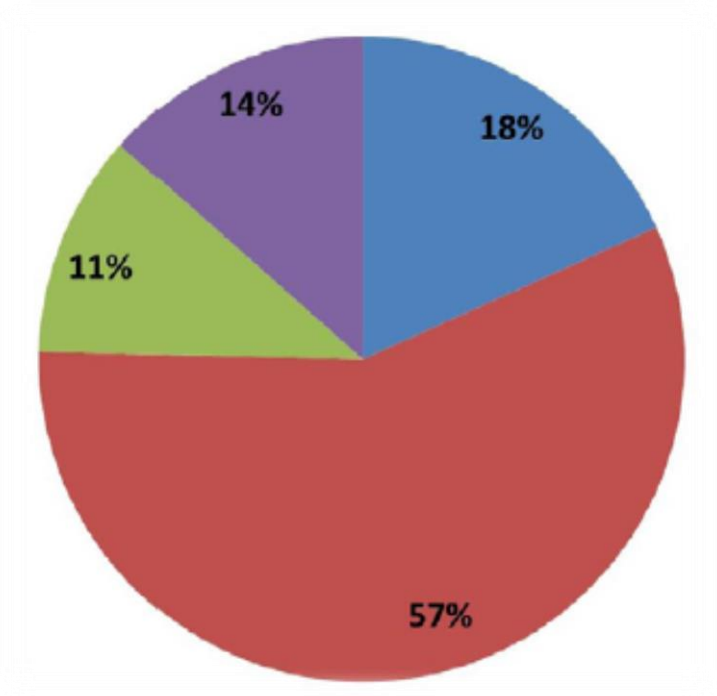
Note:

- Asia consists of 13 countries including: China, Indonesia, India, Japan, Korea, Kazakhstan, Macao, Malaysia, Philippines, Pakistan, Singapore, **Thailand** and Vietnam.
- Europe (excluding UK) consists of 28 countries including: Albania, Andorra, Austria, Belgium, Croatia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Greece, Ireland, Isle of Man, Italy, Jersey, Malta, Netherlands, Norway, Poland, Portugal, Romania, Russian Federation, Slovenia, Spain, Sweden, Switzerland and Turkey.

Source : *Horizon Scan 2014 Survey Report, BSI*

Investment in business continuity

Investment is being maintained at current levels for the vast majority of organizations.



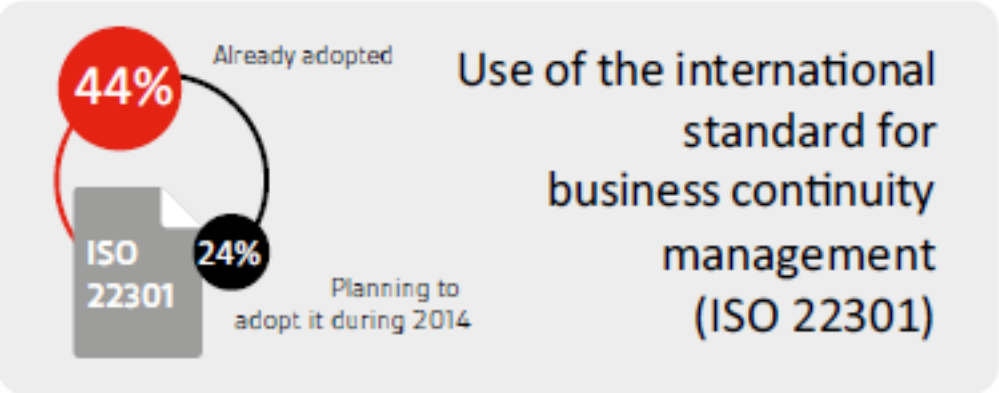
18% of organizations are increasing their budget (compared to 22% in the previous survey)
11% are actually decreasing their budget (compared to 14% in the previous survey).

Source : *Horizon Scan 2014 Survey Report, BSI*

Note: There are variations in this pattern depending on the primary activity, geographical location and size of the organization.

ISO22301 as a framework for BCM program

Less than a half of respondents (44%) currently use ISO 22301 as a framework for their BCM program although about a quarter (24%) claimed they were planning to adopt it as a framework during 2014.



Source : Beyond recovery, *BSI whitepaper for business*

Reiterating four key drivers for business leaders to implement ISO 22301 – customer confidence, reputational risk, market share loss, and governance expectations – BCI's Lyndon Bird urges companies to make the most of ISO 22301 and steal a competitive advantage. "It makes sense to have a robust BCM system, get it certified and give confidence to your stakeholders," he concludes

The benefits of implemented ISO 22301

Risk Management

86% believe BCM planning improves business resilience*

=

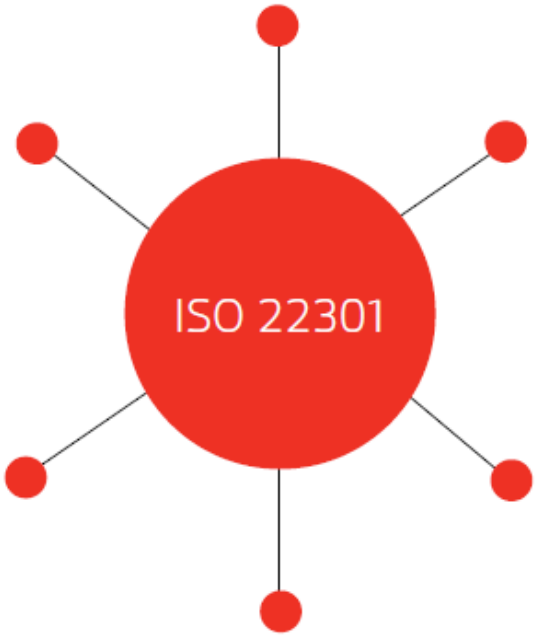
Improved mitigation of risks and robust platform for continued operation

Business Recovery

82% reported improved speed of recovery from incidents and disruptions**

=

Improved continuity of business operations and ability to provide a seamless product/service to customers in the case of unexpected disruptions



Financial Performance

71% reported increased revenue (gained from new business and customers as well as retention of existing customers)*

=

Improved commercial health and growth of the business

Operational Improvements

87% activating BCM arrangements said that they effectively reduced business disruptions*

=

Organization is better placed to foresee and prevent disruptions through Business Impact Analysis

Corporate Reputation

83% cite enhanced reputation and image amongst key stakeholders (including clients and shareholders)**

=

Improved confidence and external image as a reputable and reliable supplier

Cost-benefit Gains

81% confirmed that the cost of developing BCM plans was justified by the benefits*

=

Reduced costs associated with downtime and disruption

Source : *Need to protect your business from potential disruption, BSI*

Take away points

*"**No company is immune from business disruption**, so it's important that your organization is well-equipped to effectively minimize the disruption to your business."*

1 Identify critical business functions

Mitigate this risk by identifying your critical operations and applying a methodical approach to the threats that are posed to them

2 Produce a plan

Make a plan considering the seven 'P's needed to keep your business operational: providers (internal and suppliers), performance (service level agreements you need to meet), processes, people, premises, profile (your brand) and preparation.

3 Document your plan

Plans for disruption should never remain in the mind of the Managing Director alone.

4 Communicate

Don't let your plan gather dust on a shelf. Ensure plans are communicated, understood and made available to key staff.

5 Test your plans

Exercise your business continuity plans in mock scenarios to ensure roles and responsibilities are clear and that any flaws are exposed

6 Your suppliers need BCM too

While lean and efficient supply chains make good economic sense, unexpected events can have a significant impact on the operations and reputation of businesses. To avoid this, identify your 'critical' suppliers and ensure they have business continuity arrangements in place

7 Ensure continual improvement

Business continuity plans should be nimble and continually improving. If your plans haven't been reviewed for a few years then they probably won't meet current requirements.

8 Align to organizational objectives

Make sure your plans allow you to get back up and running in a way that aligns with your organization's objectives.

9 Insure your organization

Unexpected disruption can have a huge cost to business, so insure your organization against worst case scenarios.

10 Have an incident communications plan

Have a business continuity plan in place, so that once the situation has been assessed, a nominated senior spokesperson can communicate a strong message to your stakeholders. Reinforcing confidence in your organization's ability to recover is half the battle in business continuity.

Source : *Business continuity management, top ten tips, BSI*


Thank You!