BUSINESS CONTINUITY PLANNING

Dr. Szenes Katalin, CISA, CISM, CGEIT, CISSP, PhD
Óbudai Egyetem, Neumann János Informatikai Kar
szenes.katalin@nik.uni-obuda.hu

Business Continuity Plan

I. Definitions

II. The involvement of risk management

III. On the Components of the Information Systems Business Continuity Plan

IV. The IS BCP of the Individual Systems

I. Definitions

1. Business Continuity Planning

The purpose of business continuity planning is to enable a business to continue operations should any kind of disturbance arise.

(permanent suggestion from 1989
as Expert Reviewer of the CISA Review Manual)

1. Business Continuity Planning

Rigorous planning and commitment of resources is necessary to adequately plan for such an event. Business continuity planning is primarily the responsibility of senior management as they are entrusted with the safeguarding of both the assets and the viability of the company.

1. Business Continuity Planning

The business continuity planning is to take into consideration:

- those key operations that are utmostly necessary to the survival and later to the market success of the organizations
- the human / material resources supporting them.

1. Business Continuity / Disaster Recovery Plan

The whole business continuity / disaster recovery plan includes:

- the operations plan that is to be followed by the business units to "get by" *while* recovery is taking place *and*
- the disaster recovery plan that is generally the plan to be followed by the business units to *recover* a harmed / demolished facility or business functionality, or an operational facility

2. Information Systems Business Continuity Planning / Information Systems Disaster Recovery Plan

Everything is the same as in the case of the Business Continuity / Disaster Recovery Plan with the exception that the continuity of the information systems processing is threatened. Information systems processing is *one* operations of many that keep the organization not only alive but also successful thus it is of strategic importance.

2. Information Systems Business Continuity Planning / Information Systems Disaster Recovery Plan

Throughout the planning process of business continuity the overall plan of the organization should be taken into consideration. All IS plans must be consistent with and support the corporate business continuity plan.

II. The involvement of risk management

II. The involvement of risk management

The management classifies not only according to sustainability but successful development

- strategic goals
- ↓ business goals
- ↓ contributing processes - IT too
- ↓ contributing resources
  - human
  - material assets

The involvement of risk management

risk (resource) ~
strategic importance (resource) *
probability of *successful* attack (resource)

other factors:

- intention of the competitor or enemy
- maintenance

mitigation / elimination: management decision
Business Impact Analysis

The European Banking Association has the same opinion:

- "Financial institutions should classify the identified business functions, supporting processes and information assets"
- "To define the criticality of these identified business functions, supporting processes and information assets, financial institutions should, at a minimum, consider the confidentiality, integrity and availability requirements"
- "There should be clearly assigned accountability and responsibility for the information assets"
- "Financial institutions should review the adequacy of the classification of the information assets and relevant documentation, when risk assessment is performed"

European Banking Association Guidelines EBA /GL /2019/04
28 November 2019 - enters into force: 30 June 2020

The involvement of IT into risk management:

- "The management body has overall accountability for setting, approving and overseeing the implementation of financial institutions' ICT strategy as part of their overall business strategy as well as for the establishment of an effective risk management framework for ICT and security risks"
- "The management body should ensure that financial institutions have adequate internal governance and internal control framework in place for their ICT and security risk"
- "The management body should ensure that financial institutions have adequate internal governance and internal control framework in place for their ICT and security risks. The management body should set clear roles and responsibilities for ICT functions, information security risk management, and business continuity, including those for the management body and its committees" (EBA final report)

III. On the Components of the Information Systems Business Continuity Plan

- considerations only!

III. On the Components of the Information Systems Business Continuity Plan

Infrastructure

- Hot, Warm or Cold Site
- Alternative Hardware
- Backup of Required Supplies
- Telecommunication Networks

III. On the Components of the Information Systems Business Continuity Plan

- Servers, Storage
- Offsite Libraries and Library Controls
- Security and Control of Offsite Facilitie
- Media and Documentation Backup
- etc.

III. On the Components of the Information Systems Business Continuity Plan

Important Components of the IS BCP

- Detailed Plan
- Organization and Assignment of Responsibilities
- Emergency Response Team
- Key Decision-making Personnel
- Insurance

● / ●

III. On the Components of the Information Systems Business Continuity Plan

- Recovery/Continuity Plan Testing - plan and actual tests
- Documentation of Results
- Results Analysis
- Recovery/Continuity Plan Maintenance
- Periodic Backup Procedures
- Record Keeping for Offsite Storage

IV. The IS BCP of the Individual Systems

IV. The IS BCP of the Individual Systems

- The description of the system
- The members of the emergency team
- The key users
- The place of the systems documentation
- The databases
- The archives

IV. The IS BCP of the Individual Systems

- The typical operations fallbacks
- Manual / alternative operations
- Software & hardware environment requirements
  - current, minimum
- Communications requirements
- Recovery to normal state

References

ISACA - Information Systems Audit and Control Association
founded in: 1969 - the knowledge center of ISACA: ISACF

- ISACA Journal
  sometimes the title changes

- reference manuals: CISA, CISM, etc.:

1998 - 2019 CISA Review Technical Information Manual
published yearly;
editor: ISACA

COBIT
the methodology: Control Objectives for Information Technology

- COBIT 5, 2012, Proc.] Enabling Processes COBIT® 5:
  An ISACA Framework

References

- [COBIT 5, 2012, Proc.] Enabling Processes COBIT® 5:An ISACA Framework
  Copyright © 2012 ISACA
  ISBN 978-1-60420-239-7

- [COBIT 5, 2012, Gov.] COBIT® 5: A Business Framework for the Governance and Management of Enterprise IT
  Copyright © 2012 ISACA
  ISBN 978-1-60420-237-3

- [COBIT 2019, 2018, Gov] COBIT 2019 Framework: Governance and Management Objectives
  ISBN 978-1-60420-728-6
  Copyright © 2018 ISACA

- [COBIT 2019, 2018, Intro] COBIT® 2019 Framework: Introduction and Methodology
  ISBN 978-1-60420-644-9
  Copyright © 2018 ISACA

References

- ISO 24762 disaster recovery
- ISO 22301 business continuity management

- NIST: National Institute of Standards and Technology, USA, Department Commerce
  https://www.nist.gov

who am I?

CISA – Certified Information Systems Auditor	designator: ISACA
CISM - Certified Information Security Manager	designator: ISACA
CGEIT - Certified in Governance Enterprise IT	designator: ISACA
CISSP - Certified Information Security Professional	designator: ISC2

ISC2: International Information Systems Security Certification Consortium, founded in the USA, www.isc2.org

ISACA: information Systems Audit and Control Association, founded in the USA www.isaca.org

- lectures at the Hungarian CISA Review Course from 1999
- 1999-2019 member of the Quality Assurance Team as Expert Reviewer of the CISA Review Technical Information Manual © ISACA
- member of the Subject Matter Expert Team, as Expert Reviewer
  - COBIT 5
  - COBIT 2019