DEUTSCHE BUNDESBANK
EUROSYSTEM

Business Continuity Management (BCM) in the Bundesbank

October 2015, Christoph Stute

Definition comparison of CM and BCM

ERM/Operational Risk Management

- ERM is the overall process for early identification, handling and monitoring of risks
- ERM includes business and operational risks
- ERM gives an overview on all risks and helps to decide which risks are acceptable and which not
- ERM/ORM has preventive character

Crisis Management

- CM is the ability of an organisation to respond to any crisis situation in a predefined way
- CM includes a "tool box" with organisational and technical utilities to support management (BCP is one of the "tools")
- CM has mainly reactive character

Business Continuity Management

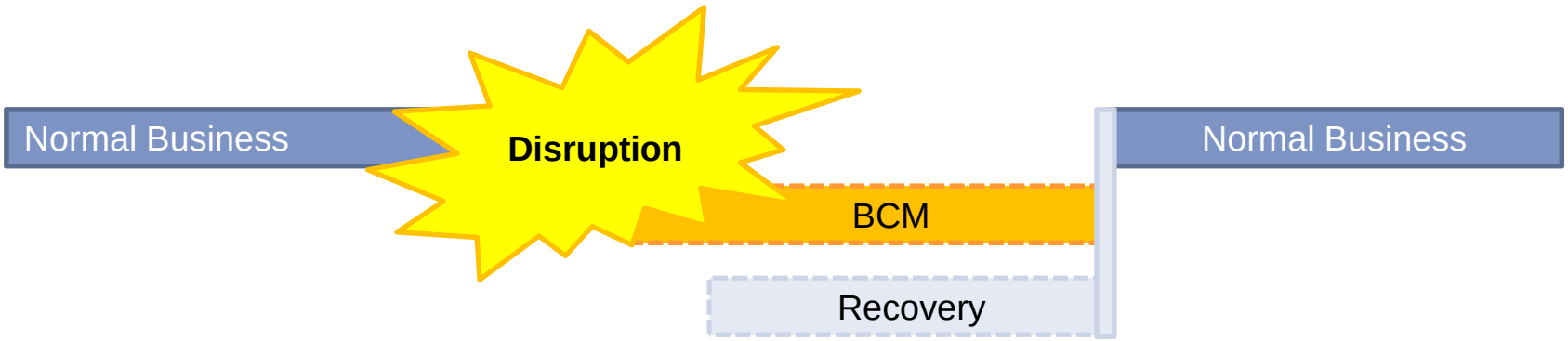
- BCM identifies potential threats to an organisation and the impacts to its most critical functions
- BCM includes BCP that put an organisation in a position to manage permanent continuity or adequate recovery of critical functions in the event of crisis situations in a predefined way.
- BCM has mainly reactive character

Definition and objective of BCP

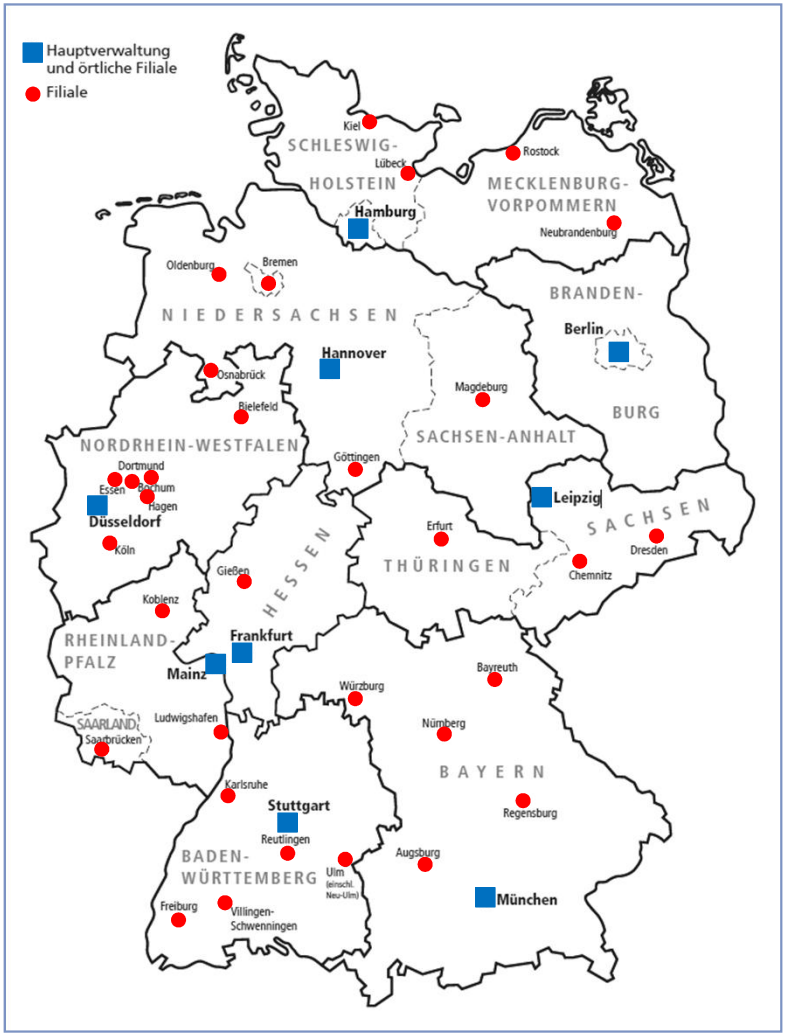
- In general Business continuity planning (BCP) aims at a temporary or possibly permanent **continuation of business operations** in emergency and disaster situations

- The objective of the Bundesbank's BCP is the **continuation of key central bank business activities** in emergency and disaster situations, in order to avoid the central bank causing a destabilisation of the financial system

- Consideration given to risk and cost-benefit aspects



Bundesbank´s structure



Central Office in Frankfurt

Executive Board: President, Vice-President, other 4 members

Principle policy and strategic issues

9 regional offices

Bundesbank representation, service centres, operational tasks (especially banking supervision)

38 branches

Money processing, cash distribution

History of BCM at Bundesbank

- BCM is not a new issue for the Bundesbank; contingency measures have been in place since its early days

- But in the past BCM wasn’t a major issue, because of
  - relying on manual procedures for performing business,
  - the decentralised organizational structure and decentralised execution of business (most of critical functions were performed on regional level) leading to a broad protection against major incidents,
  - technical redundancies through decentralised data centres.

Reasons for investigation and strengthening Business Continuity Planning

External events

- Year 2000
- Terrorism, 9/11
- Serious power supply failures in North America and Europe in 2003
- Computer viruses: My doom, Sober …
- Contingency obligations (e.g. TARGET security Requirements, KRITIS, Basel II, Act on Corporate Governance and Transparency…)

Internal reasons

- In-house power supply failures
- Structural reform former decentralised crisis and business continuity management organisation obsolete

Development of BCM at the Bundesbank

1. **Business Impact Analysis** (BIA) to identify most critical business functions / processes
   → definition of core business function (s. next slides)

2. Analysis of potential threats
   → definition of **scenarios** to be responded to (s. next slides)

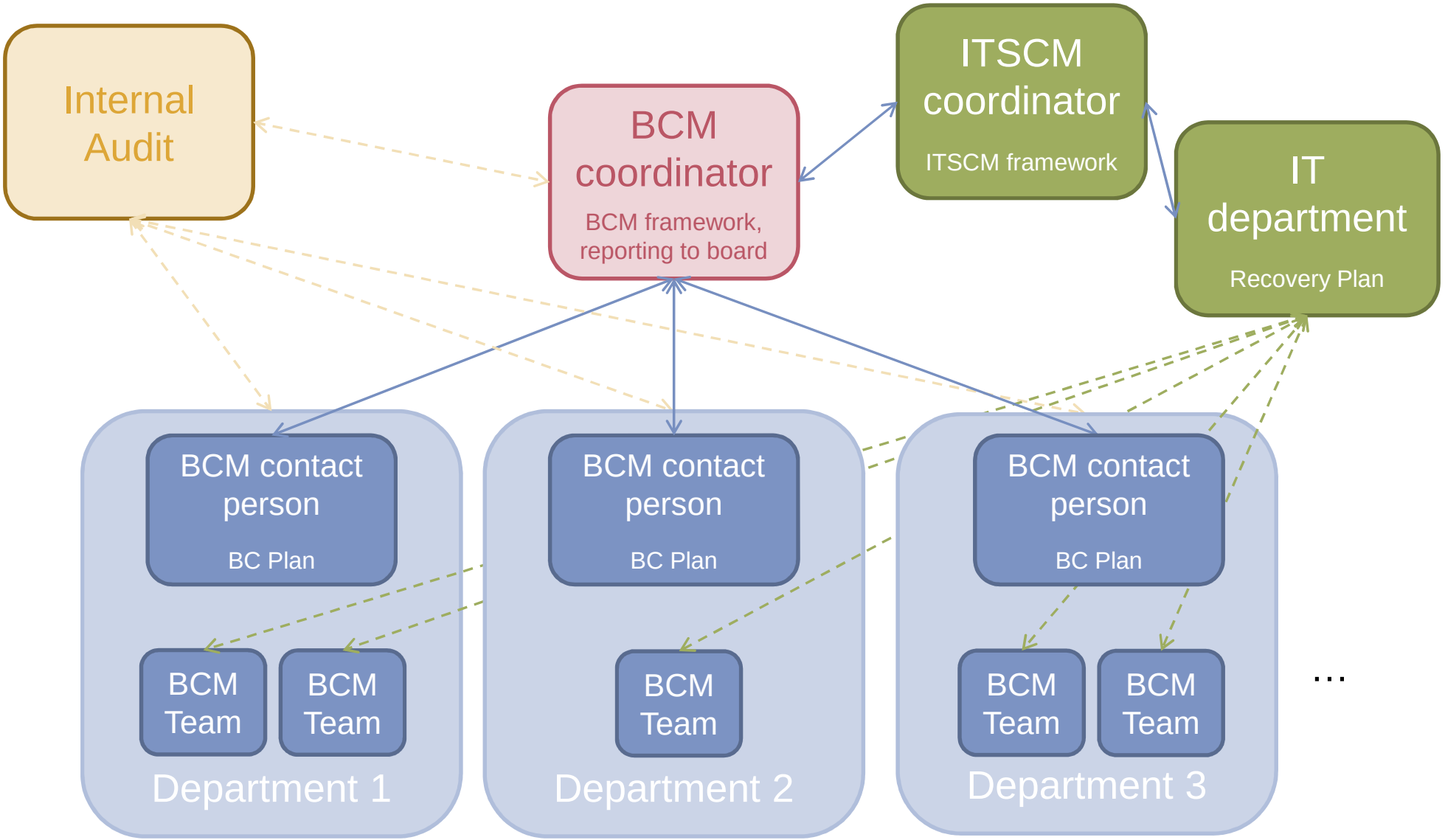
3. Board decision which function / process has to be **secured against which threat** on basis of a cost/benefit analysis by the board

4. Identification of organisational and technical **measures** to reach safeguarding (BC plans)

Roles and responsibilities

- BCM strategy ☞ Ex. Board
  = decision on definition of 1) to 3)
- BCP (developing and implementation) ☞ business units on basis of the predefined scenarios
- BCP (methodology and reporting) ☞ Division Organisation, Security and Crisis Management Section

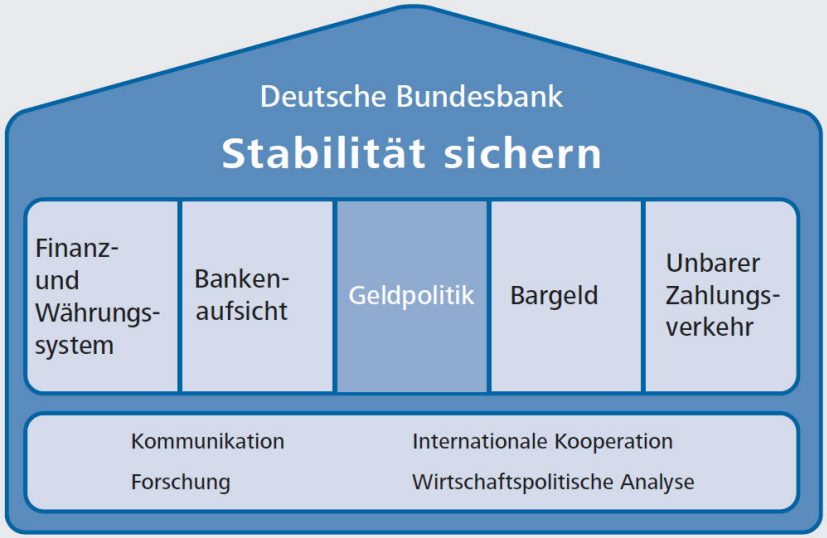
Bundesbank BCM Governance



Critical core business areas of the Deutsche Bundesbank

- Cash and cashless payments
- Operational monetary policy including collateral management
- Account management and accounting
- Foreign exchange and reserve management for the Bundesbank and on behalf of the ECB
- not statistics, banking supervision or research

Bundesbank Strategy 2016



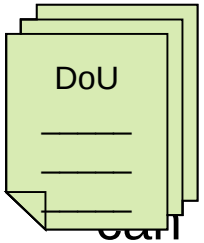
Scenario technique

Scenario 1	Staff available, premises available, cluster of datacentre (incl. communication service) temporarily unavailable ☞ Hot secondary site
Scenario 2	Staff available, essential site(s) partially unavailable, cluster of datacentre (incl. communication service) available ☞ Splitted units continue working and use of remote access/teleworking
Scenario 3a	Staff available, essential site(s) unavailable, cluster of datacentre (incl. communication service) unavailable ☞ Splitted units continue working and use of remote access/teleworking ☞ hot secondary site
Scenario 3b	Staff unavailable at one location, essential site(s) unavailable, cluster of datacentre (incl. communication service) unavailable ☞ Hot secondary site ☞ Splitted units continue working
Scenario 4	Staff unavailable at one location, essential site(s) unavailable, both datacentre (incl. communication service) unavailable, entire region with customers and partners is similarly affected → No decision to safeguarded scenario 4
Scenario Pandemic	Loss of staff up to six months that starts with an unavailability of few employees but can in the extent mean that 30 % of the staff are not available

Implementation of Business Continuity Planning (Part I)

- Securing availability of information technology applications and data
  - Data backup
  - Installation of a second data processing center (2nd site, hot-standby)
  - Redundancy of hardware, power supply, network, …
- Securing ability to communicate for crisis management team and BCP Teams
  - Redundancy of telecommunication infrastructure
  - Fall back solutions
- Implementation of fall back procedures, if IT applications are not available

Implementation of Business Continuity Planning (Part II)



- Service Level Agreements between business units and supporting units (so that everybody exactly knows, what is expected and what be delivered)

- Installation of backup operations sites depending on organisational issues (fully equipped sites or sites normally used for other purposes which can be used by BCP-team if necessary)

- Splitting of operations staff into teams at different sites in normal times, so that one team can take over in a crisis

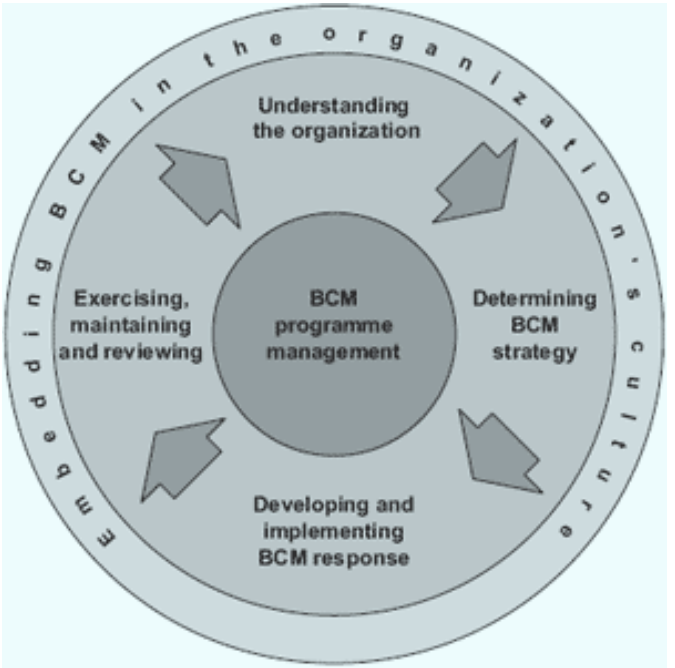
- Training of staff

- Regular testing

Development of BCM at the Bundesbank

BCM Life Cycle

- **Ongoing investigation** as processes and threats change permanently
  - To check processes by business areas and IT
  - To co-ordininate and report to Executive Board by section Security, BCM and CM
  - To review regularly by Internal Audit and external auditing firms



IT-safeguarding

- After breakdown of both data centres in 2010 Bundesbank became aware that BCPs cover only an IT breakdown what ends within one business day
- A breakdown of IT that lasts longer than one business day might have heavy effects for the business of the Bundesbank

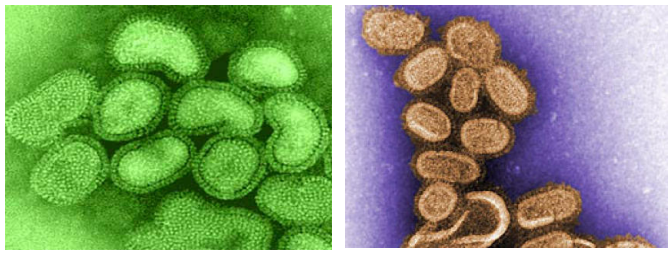
→ Implementation of telephone, fax and PC outside of the Bundesbank IT network

→ Critical business areas currently check how business can be continued if IT is not available for more than one day up to five business days (no respectively

Pandemic planning

Bundesbank general pandemic plan

- Disinfection, disinfectant spray, medical masks
- Business and staff will be reduced to the essential
- Critical business areas have documented their pandemic planning
- All business areas are asked to check their essential staff annually
- The essential staff use teleworking if possible to avoid infection on their way to work
- The essential staff check the facilities for teleworking twice a year
- Bundesbank will order vaccines for employees from the Federal Government’s supply of vaccines



Any questions???