Contingency planning
DAU Marts 2013
Agenda

- Introduction
- Process definition
- Activation and notification
- Recovery
- Reconstruction
- Evaluation
- Examples
- Do and Don’t
Contingency plan

Why bother?

Information provided by information technology systems must be based on reliable, relevant and accessible data, but before this data can add any value, the data must be transformed into knowledge based decisions and actions.

That means if data to be seen as a valuable asset then data must be protected and taken care of, analogue to any other asset management disciplines.

One instrument for data asset management is to recover IT systems quickly and effectively after an disaster has occur.

By other word if your IT systems are vital for running the business then you need to develop and implement some kind of IT contingency plan.
Contingency plan
Scope

Problem
A Problem is the unknown underlying cause of one or more Incidents

Emergency
A Incident with a high impact or potentially high impact, which requires a response that is above a normal operation

Disaster
An occurrence causing widespread destruction and disruption of the overall business processes.

Expert to analyze and solve the problem

Problem management

Incident

Emergency
Perform error handling according to current procedures

Problem

Error handling

Disaster
Initiate continuity plan and disaster team to manage the disaster

Continuity plan
Define, develop, implement and evaluate an effective contingency plan based on a phase divided process.
A contingency plan enables the organization to respond quickly and structured when an disaster occurs. Recovery time decrease by having the right tools, documentation and resources in place.

Activation of the contingency plan occurs after disruption or outage. When a disaster is detected the disaster team is established and an recovery approach is decided.

The detailed recovery activity and resource plan is execute. Current procedures and instructions are performed by skilled persons that can recover the system without intimate system knowledge.

In the reconstruction phase, temporary recovery solutions are terminated and the system is transfer back to fully normal operation mode.

Evaluation of how durable the contingency plan is to support high recovery performance based on test and review activities.
Contingency plan

Definition

Process definition
- Introduction
- Scope
- Responsibilities
- Process overview
- Business impact
- Risk assessment

Activate and notify

Recovery

Reconstruction

Evaluate
Contingency plans
Roles and responsibilities

- Disaster team
  - System owner
  - System manager
  - System experts
  - Process experts
  - Service providers

- Planning
  - System recovery
  - Business continuity

- Communication
  - Business managers
  - System users
  - Extern parties

- Recover activities
  - Toolbox
    - Establish Infrastructure
    - Install and configure server
    - Install and configure clients
    - Test and operate
    - Backup system and data

<table>
<thead>
<tr>
<th>Role</th>
<th>Define</th>
<th>Activate &amp; notify</th>
<th>Restore</th>
<th>Reconstruct</th>
<th>Evaluate</th>
</tr>
</thead>
<tbody>
<tr>
<td>System owner</td>
<td>A</td>
<td>A</td>
<td>I</td>
<td>I</td>
<td>A</td>
</tr>
<tr>
<td>System manager</td>
<td>R</td>
<td>R</td>
<td>A</td>
<td>A</td>
<td>R</td>
</tr>
<tr>
<td>PIT manager</td>
<td>C</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>C</td>
</tr>
<tr>
<td>Disaster team member</td>
<td>C</td>
<td>C</td>
<td>I</td>
<td>I</td>
<td>R</td>
</tr>
<tr>
<td>System expert</td>
<td>I</td>
<td>I</td>
<td>R</td>
<td>R</td>
<td>C</td>
</tr>
<tr>
<td>Process expert</td>
<td>I</td>
<td>I</td>
<td>R</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td>Site coordinator</td>
<td>C</td>
<td>I</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Super Users</td>
<td>C</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>C</td>
</tr>
<tr>
<td>Users</td>
<td>I</td>
<td>I</td>
<td>R</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td>Global IT</td>
<td>C</td>
<td>I</td>
<td>R</td>
<td>R</td>
<td>C</td>
</tr>
<tr>
<td>PIT support</td>
<td>I</td>
<td>I</td>
<td>C</td>
<td>C</td>
<td>I</td>
</tr>
<tr>
<td>Service provider</td>
<td>I</td>
<td>I</td>
<td>C</td>
<td>C</td>
<td>I</td>
</tr>
</tbody>
</table>

A - accountable, R - responsible, C - contributor, I - informed
## Contingency plan

### Business impact

<table>
<thead>
<tr>
<th>Process</th>
<th>Impact</th>
<th>MTD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forecast</td>
<td>Missing demand plan</td>
<td>5 days</td>
</tr>
<tr>
<td>Schedule</td>
<td>No order scheduled</td>
<td>3 days</td>
</tr>
<tr>
<td>Shipment</td>
<td>Goods not issued</td>
<td>1 day</td>
</tr>
<tr>
<td>Release</td>
<td>Batch is not released</td>
<td>2 days</td>
</tr>
<tr>
<td>Review</td>
<td>Batch is not reviewed</td>
<td>3 days</td>
</tr>
<tr>
<td>Recipe</td>
<td>Recipe issues</td>
<td>2 days</td>
</tr>
<tr>
<td>Execute</td>
<td>Production shortage</td>
<td>1 day</td>
</tr>
</tbody>
</table>

### Maximum Tolerable Downtime

- **System**
  - SAP: 2 days, 24 Hours
  - LIMS: 1 day, 8 Hours
  - BO: 5 days, 48 Hours
  - MES: 1 day, 8 Hours
  - PCS: 8 hours, 2 Hours

### Recovery Time Objective

- **System**
  - SAP: 2 days, 24 Hours
  - LIMS: 1 day, 8 Hours
  - BO: 5 days, 48 Hours
  - MES: 1 day, 8 Hours
  - PCS: 8 hours, 2 Hours

### Recovery Point Objective
Contingency plan
Risk Assessment

LIMS

Printer

SAP

Batch executor

Batch

PCS

OFC Hub

App server

D server

DANGER
THIN ICE
Contingency plan
Risk assessment

<table>
<thead>
<tr>
<th>No</th>
<th>Disaster</th>
<th>Consequences</th>
<th>Basic control</th>
<th>Mitigations</th>
<th>Recovery strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fire outbreak</td>
<td>Server is inaccessible</td>
<td>Fire protection inspection</td>
<td>Fire extinguisher</td>
<td>Warm system swop</td>
</tr>
<tr>
<td>2</td>
<td>Power supply</td>
<td>Uncontrolled server shut down</td>
<td>Unbreakable power supply</td>
<td>Redundant power supply</td>
<td>Warm system swop</td>
</tr>
<tr>
<td>3</td>
<td>Virus attack</td>
<td>System malfunction</td>
<td>Virus protection</td>
<td>Firewalls</td>
<td>Isolate network area and operate manual until virus is removed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Operation system patching</td>
<td>Separated network</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Network failure</td>
<td>Data loss</td>
<td>Updated documentation</td>
<td>Redundant network</td>
<td>Hot system swop</td>
</tr>
<tr>
<td>5</td>
<td>Room condition don't work</td>
<td>Low system performance</td>
<td>Preventive maintenance</td>
<td>Room surveillance</td>
<td>Contact vendor and wait until the room temperature is normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Service agreement</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Break down</td>
<td>Control system is damage</td>
<td>Updated baseline</td>
<td>System surveillance</td>
<td>Exchange equipment and restore application</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Spare part on stock</td>
<td>Incident process in place</td>
<td></td>
</tr>
</tbody>
</table>

Impact
- Critical
- Major
- Moderate
- Minor

Likelihood
- Unlikely
- Possible
- Likely
- Very Likely

Gross risk
Basic risk
Net risk

Difference between Gross, basic and Net risk
Contingency plans
Activate and notify

- Process definition
- Activate and notify
  - Detect disaster
  - Gather information
  - Notify
  - Establish team
  - Priorities actives
  - Communicate
- Recover
- Reconstruct
Contingency plan
Disaster recovery plan

Activate and Notify
- Assess
- Notify
- Plan
- Inform
- Recover

Recovery
- Verify
- Reconstruct
- Qualify
- Operate

Reconstruction
- Evaluate
Contingency plan
Disaster recovery plan

Access
Gather information and establish a status overview of the disaster
System manager

Notify
Notify the disaster team and initiate the first planning meeting
System owner

Plan
Based on the disaster impact a prioritized activity plan is created
Disaster team

Inform
Identify effected key stakeholders and inform about the disaster situation and the planed activities
System owner

Recover
Reestablish faulty network components, exchange damaged equipment, install/config software modules and recover data
System manager

Verify
Verify through a test plan system installation, operation and performance is correct
System manager

Reconstruct
Reestablish system and all service at primary location
System manager

Qualify
Qualify through a test plan system installation, operation and performance is correct
System manager

Operation
Start the system operation and control that system operate satisfactorily and can be used as intended
System manager

Evaluate
When all the disaster activity is successfully executed the disaster process performance is evaluated and documented
System owner
Contingency Plan
Documentation in the recovery box

System documentation
- Network topology
- Configuration item list
- Installation manuals
- License files
- Software installation files

User documentation
- User manuals
- Exception guidance
- Business continuity plan

Service documentation
- Known error database
- IT continuity plan
- Backup/recover procedure
Contingency plan

Restore strategies

Resilience

Service agreement

Customer

Vendor

Contingency plan

Restore strategies

Resilience

Service agreement

Customer

Vendor

Contingency plan

Restore strategies

Resilience

Service agreement

Customer

Vendor
Contingency plan
Data recover strategies
Contingency plan
Reconstruction

- Process description
- Activate and notify
- Recovery
- Reconstruction
  - Verify operation
  - Verify performance
  - Hypecare
- Evaluate
Contingency plan
Disaster scenarios
Contingency plan

Virus attack

Situation
A virus found on a central application server was not identified by the virus scanner

Issue
The virus was polling the network to find possible other computers to attack

Consequence
Performance on many process computers was low and this has impact on the product deliveries

Action
- Isolate process net
- Close down process computers and remove virus manually
- Install new windows path
- Develop and install a new virus cure

Evaluation
Install data surveillance between administrative and process domain
Contingency plan

Upgrade

Situation
After system upgrade the system performance was very slow

Issue
The system parameter with handle the amount a services was not updated

Consequence
Information exchange with process equipment was very slow with effect the production output

Action
• Close down some lines to keep the process area running
• Manually material handling
• By analyzing the program a system parameter fault was found

Evaluation
The system parameter was added as a critical item to the configuration item list
Contingency plan

Cable

Situation
After construction work the fiber between the server room and process net was broken

Issue
No information could be exchanged between the central server and the process clients

Consequence
Order information was not downloaded and process performance information was not uploaded

Action
- Order parameter has to be typed in manually
- Performance information has to be log manually
- Information has to be reviewed by another before use
- Temporary cable repair was conducted

Evaluation
Establish redundant server room with separated fiber and switch
Contingency plan

Evaluation

- **Plan Review**
  - Does the plan account for all current critical business processes
  - Is the contact details accurate
  - Verify the completeness of the recovery plan
  - Mature disaster team
  - Sufficient skilled and trained restore individuals
  - Updated system documentation and backup procedure

- **Simulation**
  - Coordination between disaster team internally and externally
  - Quality of documentation, instructions and backup media
  - Key personnel are proper trained and skilled to manage a disaster recovery

- **Evaluate**
  - What have done right ?
  - What could have been done differently ?
  - Did we perform any not value adding activity ?
  - What shall we improve ?
Contingency plan

Do and don’t

- **Requirement**
  - Operational backup/restore procedure
  - Qualified resources available
  - Updated system documentation
  - Clarify roles and responsibilities
  - Mature change management process

- **Do**
  A formal document with can support the disaster process recovery in effective and operational way.

- **Don’t**
  “So ein ding must wir auch haben” which means that the document are only been to be written on a computer and never going to be tested or evaluated.
Appendix

- Definitions and Abbreviations
- Reference
## Contingency Plan
### Definition and Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contingency plan</td>
<td>System-specific plan developed recovering an IT system in case of Disaster</td>
</tr>
<tr>
<td>Disaster</td>
<td>An occurrence causing widespread destruction and disruption of the overall business processes (e.g. fire at the global server centre)</td>
</tr>
<tr>
<td>System recovery</td>
<td>The process of bringing the system back to operational status</td>
</tr>
<tr>
<td>Business continuity</td>
<td>The business area’s ability to operate its vital operations without the normal use of IT</td>
</tr>
<tr>
<td>Hot system</td>
<td>A fully operational redundant equipped system</td>
</tr>
<tr>
<td>Warm system</td>
<td>A partly equipped system with require some addition work to be fully operational</td>
</tr>
<tr>
<td>Cold system</td>
<td>Backup equipment with may need to be installed, configured and tested before the system is fully operational</td>
</tr>
<tr>
<td>IT service agreement</td>
<td>A agreement with specify the service provided to a customer by an IT Vendor</td>
</tr>
<tr>
<td>Resilience</td>
<td>The ability to quickly adapt and recover from any known/unknown change</td>
</tr>
<tr>
<td>MTD</td>
<td>Maximum Tolerable Downtime is amount of time a critical process can be disrupted without cause server harm to the business</td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objective is the maximum tolerated time data can be lost without huge impact on the business</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objective is the overall length of time before a breakdown has severe impact on the business</td>
</tr>
</tbody>
</table>
Contingency Plan

Reference

- IT disaster recovery planning, Dummies
- Contingency planning Guide, NIST
- Backup and recovery, DELL
- Your Backup is not an Archive, Symantec
- Forøg virksomhedens informationssikkerhed, ITEK
- IT sikkerhed i små og mellemstore virksomheder, DIT