Contingency planning

DAU Marts 2013

CHR. HANSEN

Improving food & health

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 bee seen as an valuable asset then data must be protected and taking 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.

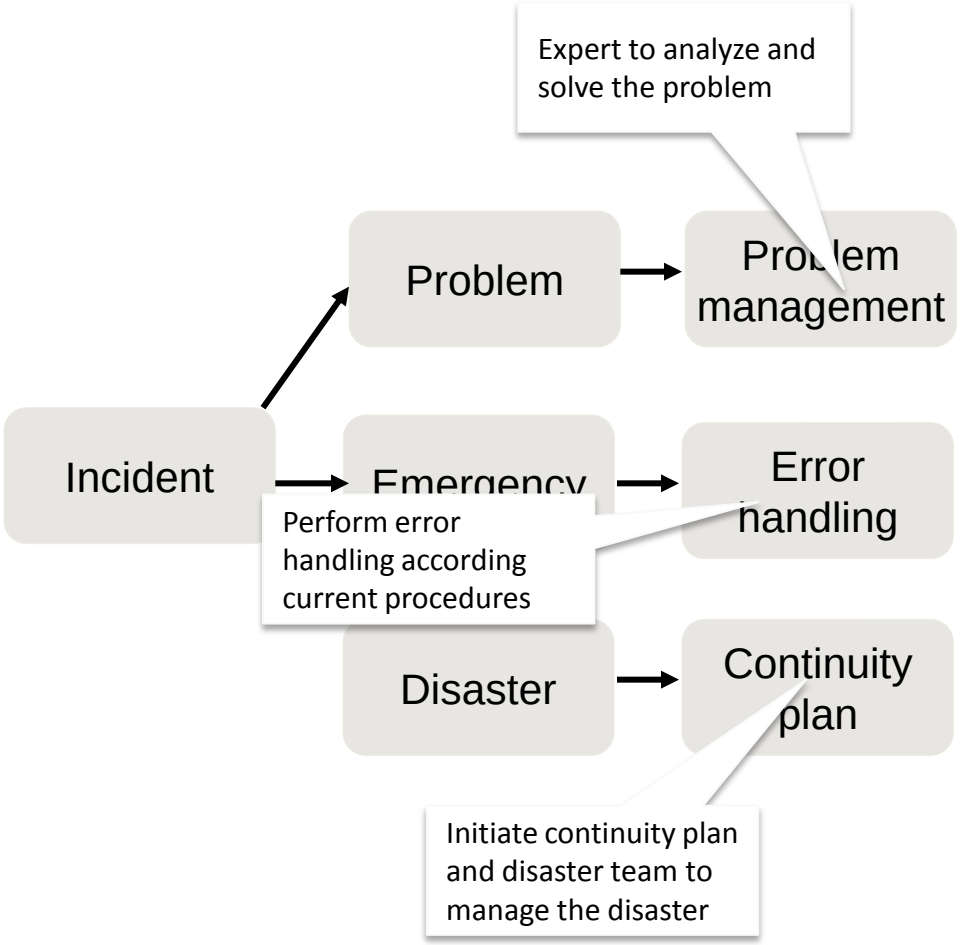
By other word if your IT systems are vital for running the business then you need to develop and implement some kind of IT contingency plan.

Contingency plan
Scope

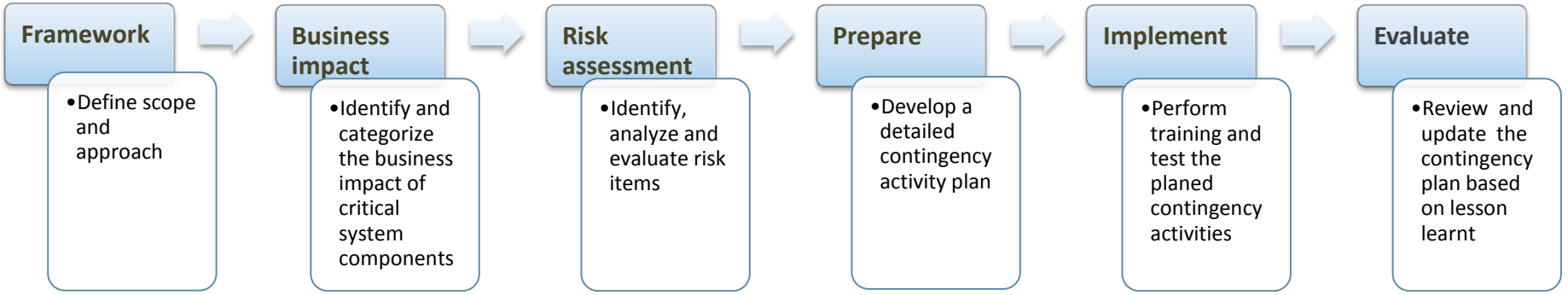
Problem
A Problem is the unknown underlying cause of one or more Incidents

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

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



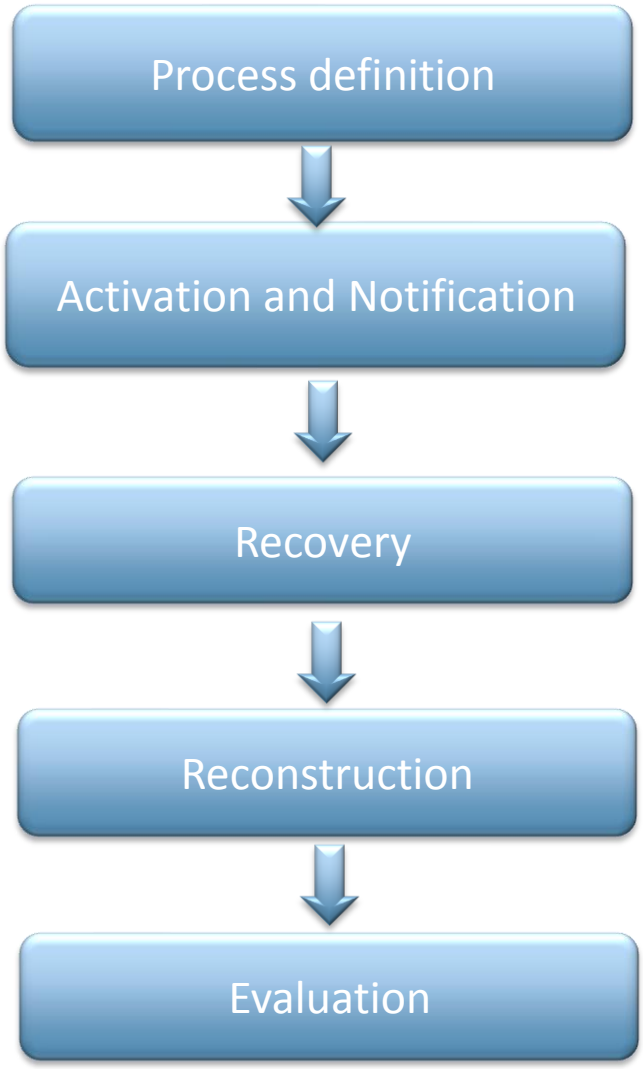
Contingency plan
Implementation roadmap



Define, develop, implement and evaluate an effective contingency plan based on a phase divided process.

Contingency plan

Content



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.

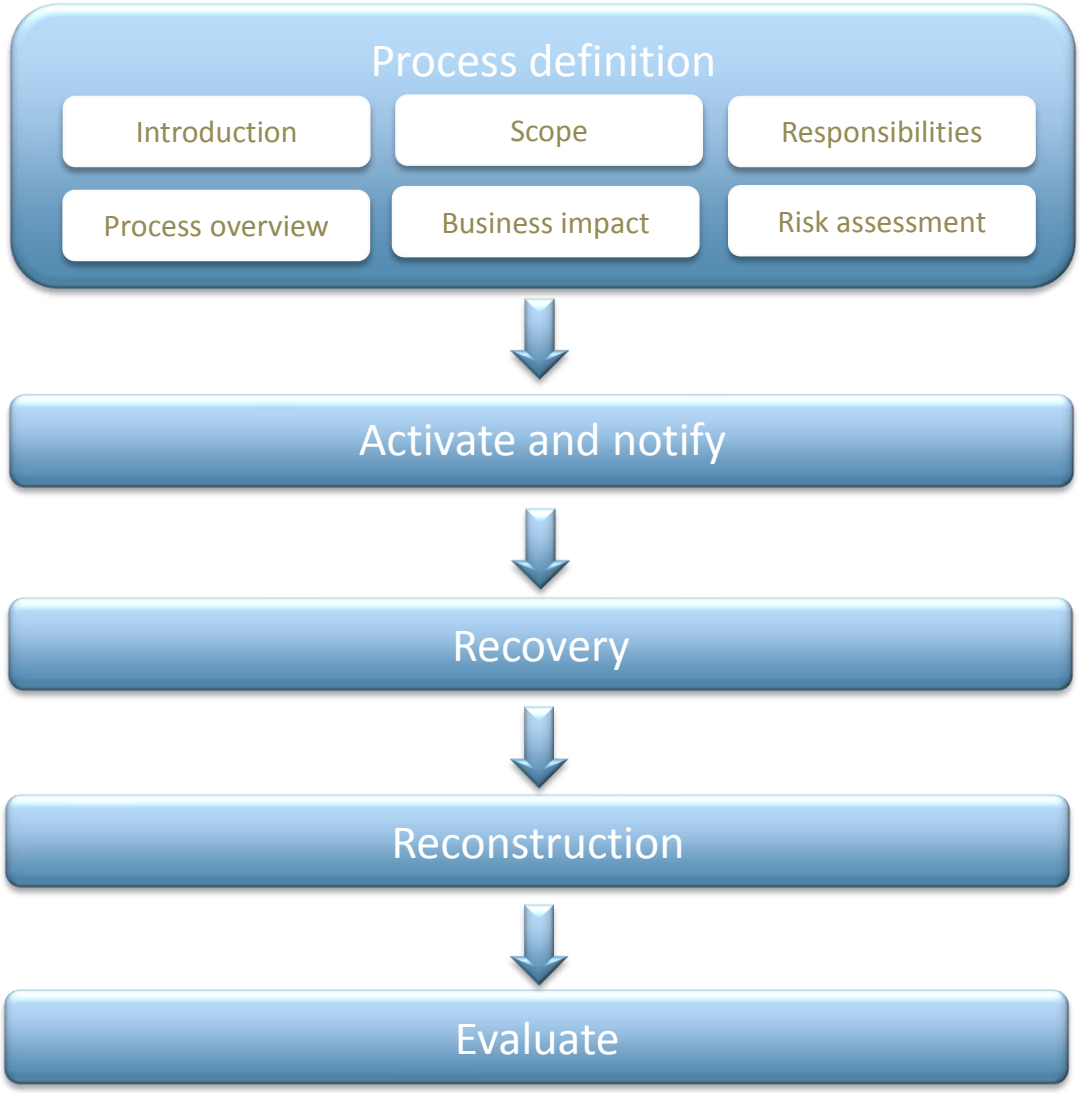
The detailed recovery activity and resource plan is execute. Current procedures and instructions are performed by skilled persons that can recover the system without intimate system knowledge.

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

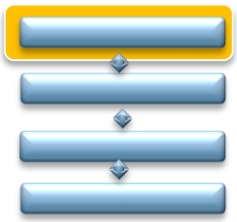
Definition



Contingency plans

Roles and responsebilities

- Disaster team
  - System owner
  - System manager
  - System experts
  - Process expetrs
  - 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



Role	PIT contingency process				
	Define	Activate & notify	Restore	Reconstruct	Evaluate
System owner	A	A	I	I	A
System manager	R	R	A	A	R
PIT manager	C	I	I	I	C
Disaster team member	C	C	I	I	R
System expert	I	I	R	R	C
Process expert	I	I	R	R	I
Site coordinator	C	I	C	C	C
Super Users	C	I	I	C	C
Users	I	I	R	R	I
Global IT	C	I	R	R	C
PIT support	I	I	C	C	I
Service provider	I	I	C	C	I
A-accountable, R - responsible, C - contributor, I – informed					

CHR. HANSEN

Contingency plan

Business impact

Maximum Tolerable Downtime

Recovery Time Objective

Recovery Point Objective

Process	Impact	MTD
Forecast	Missing demand plan	5 days
Schedule	No order scheduled	3 days
Shipment	Goods not issued	1 day
Release	Batch is not released	2 days
Review	Batch is not reviewed	3 days
Recipe	Recipe issues	2 days
Execute	Production shortage	1 day

System	RTO	RPO
SAP	2 days	[illegible] urs
LIM		
BO	5 days	48 Hours
MES	1 days	8 Hours
PCS	8 hours	2 Hours

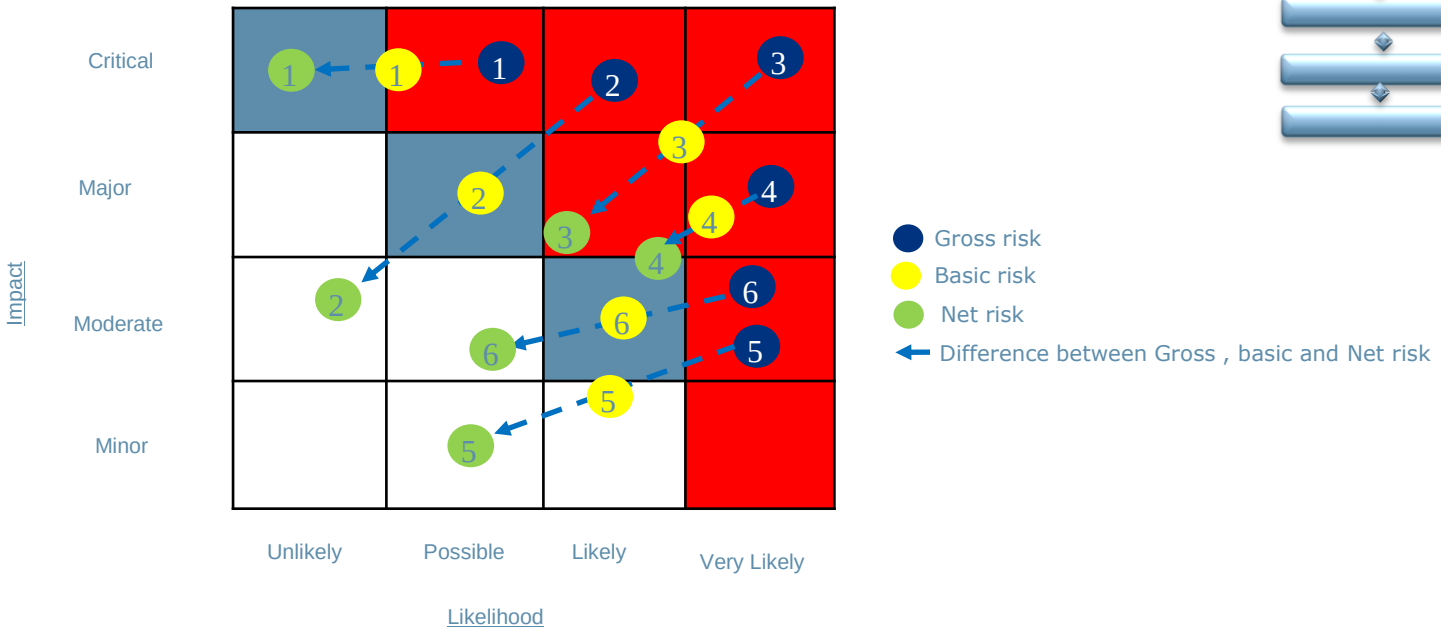
CHR. HANSEN

Contingency plan

Risk Assessment

Contingency plan

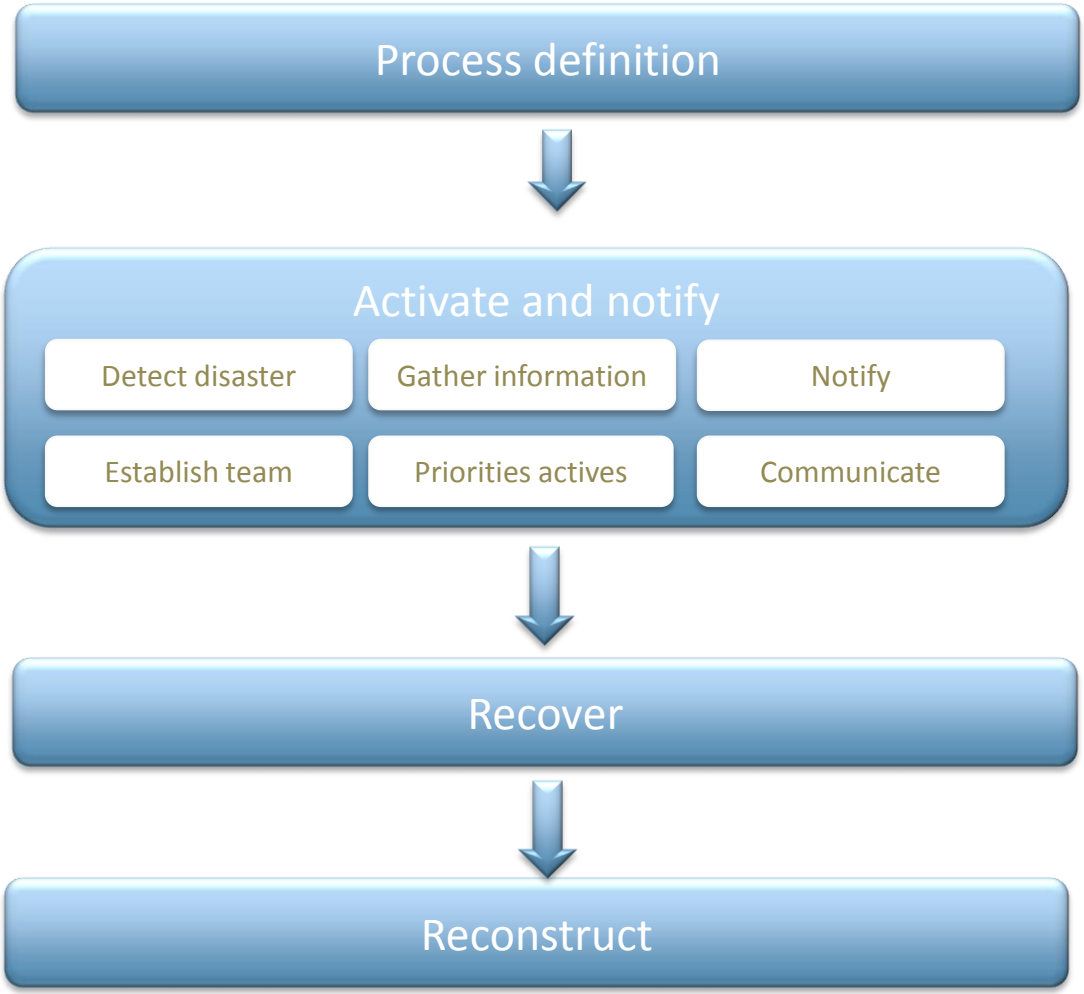
Risk assessment



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

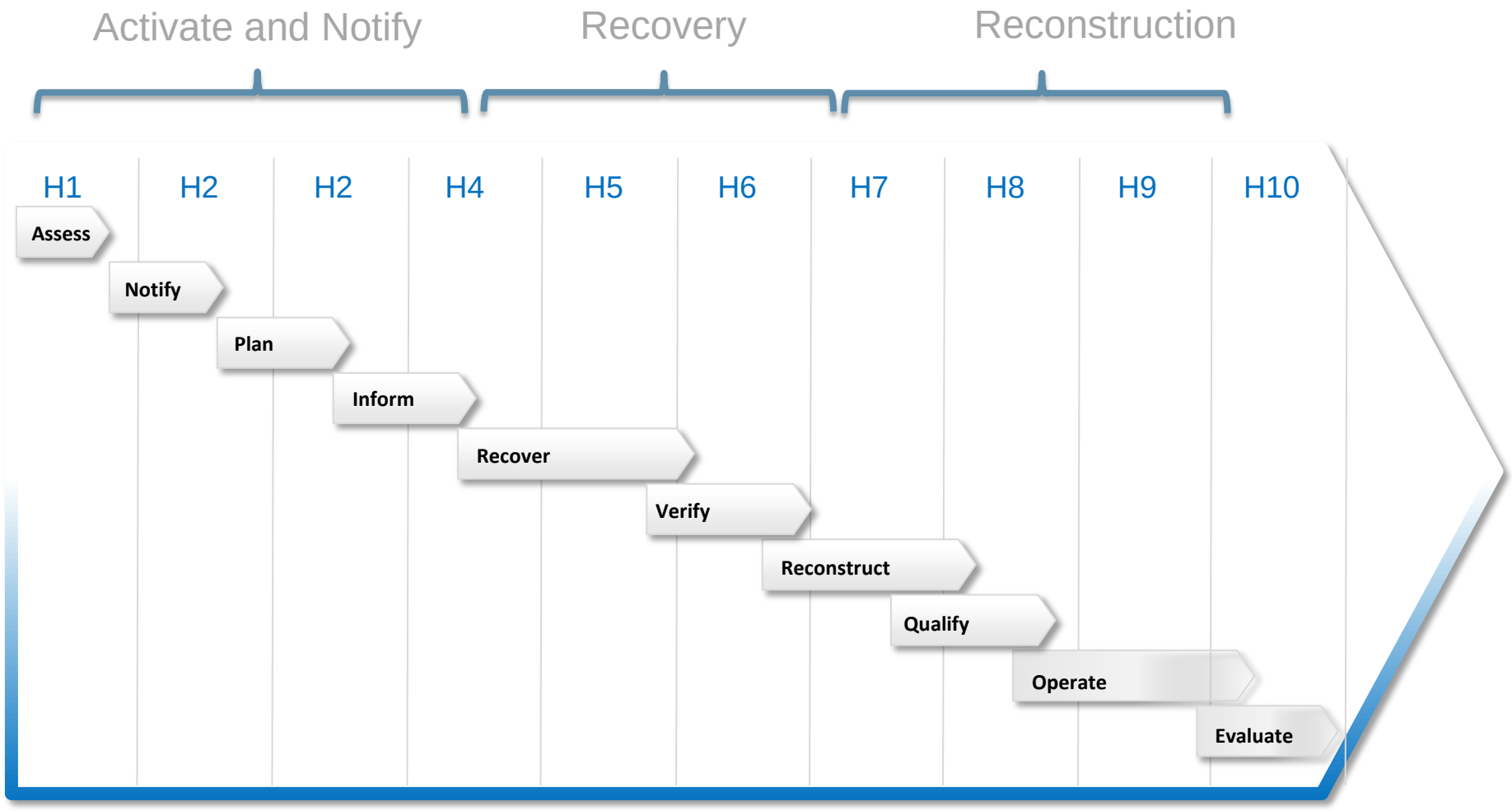
Contingency plans

Activate and notify



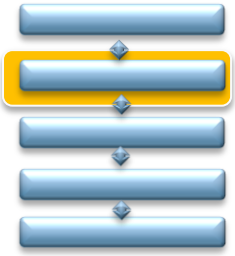
Contingency plan

Disaster recovery plan



Contingency plan

Disaster recovery plan

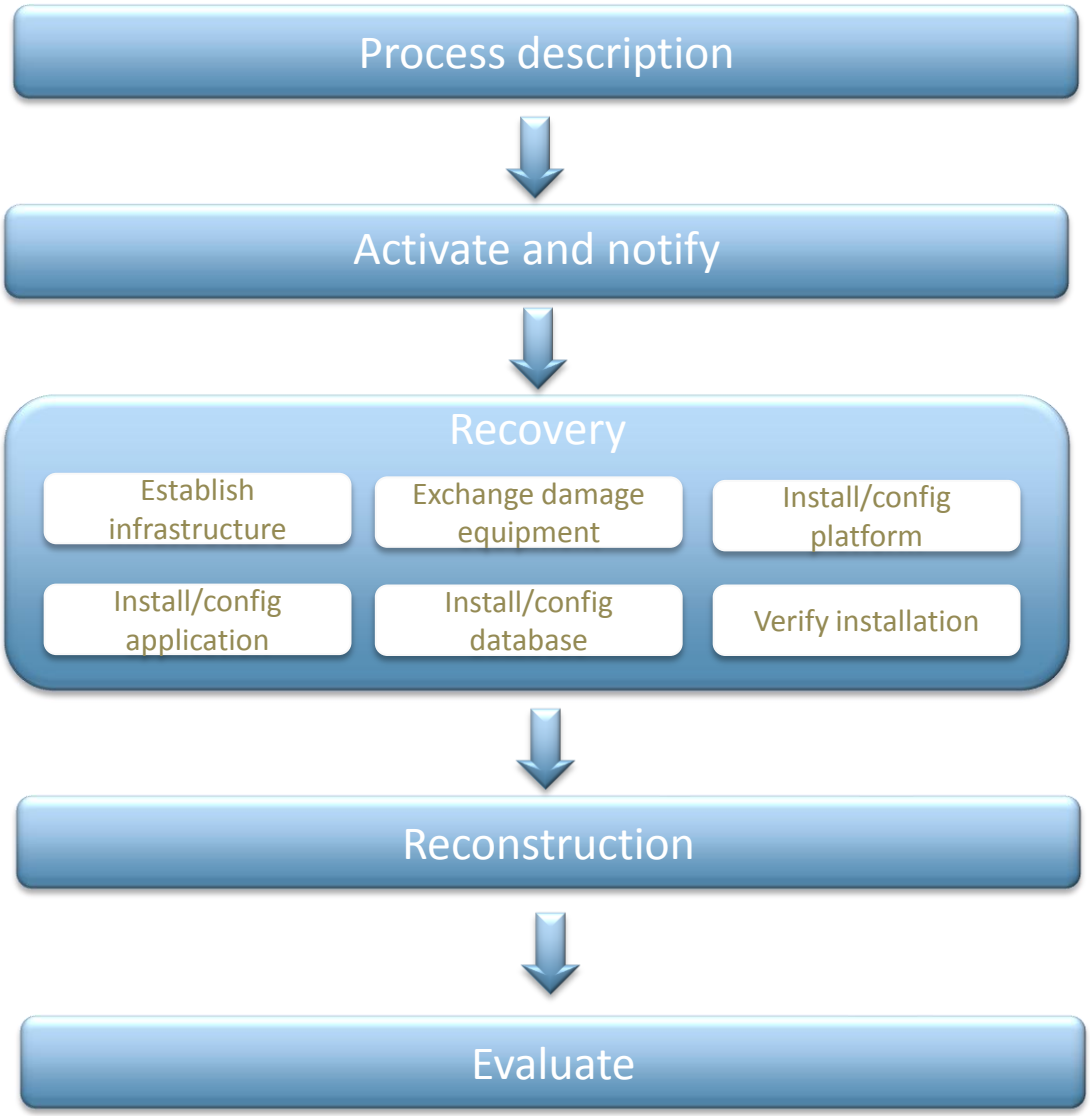


Access	Gather information and establish a status overview of the disaster	System manager
Notify	Notify the disaster team and initiate the first planning meeting	System owner
Plan	Based on the disaster impact a prioritized activity plan is created	Disaster team
Inform	Identify effected key stakeholders 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

CHR. HANSEN

Contingency plan

Recovery



Contingency Plan

Documentation in the recovery box

System documentation

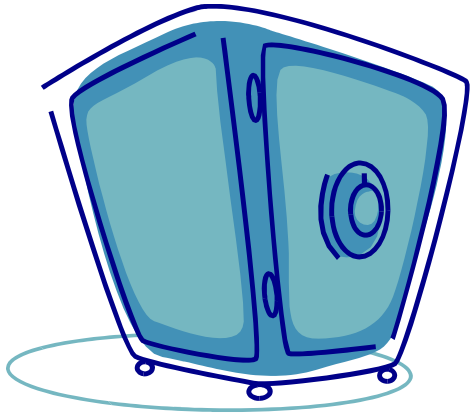
- Network tropology
- Configuration item list
- Installation manuals
- License files
- Software installation files

User documentation

- User manuals
- Exception guidance
- Business continuity plan

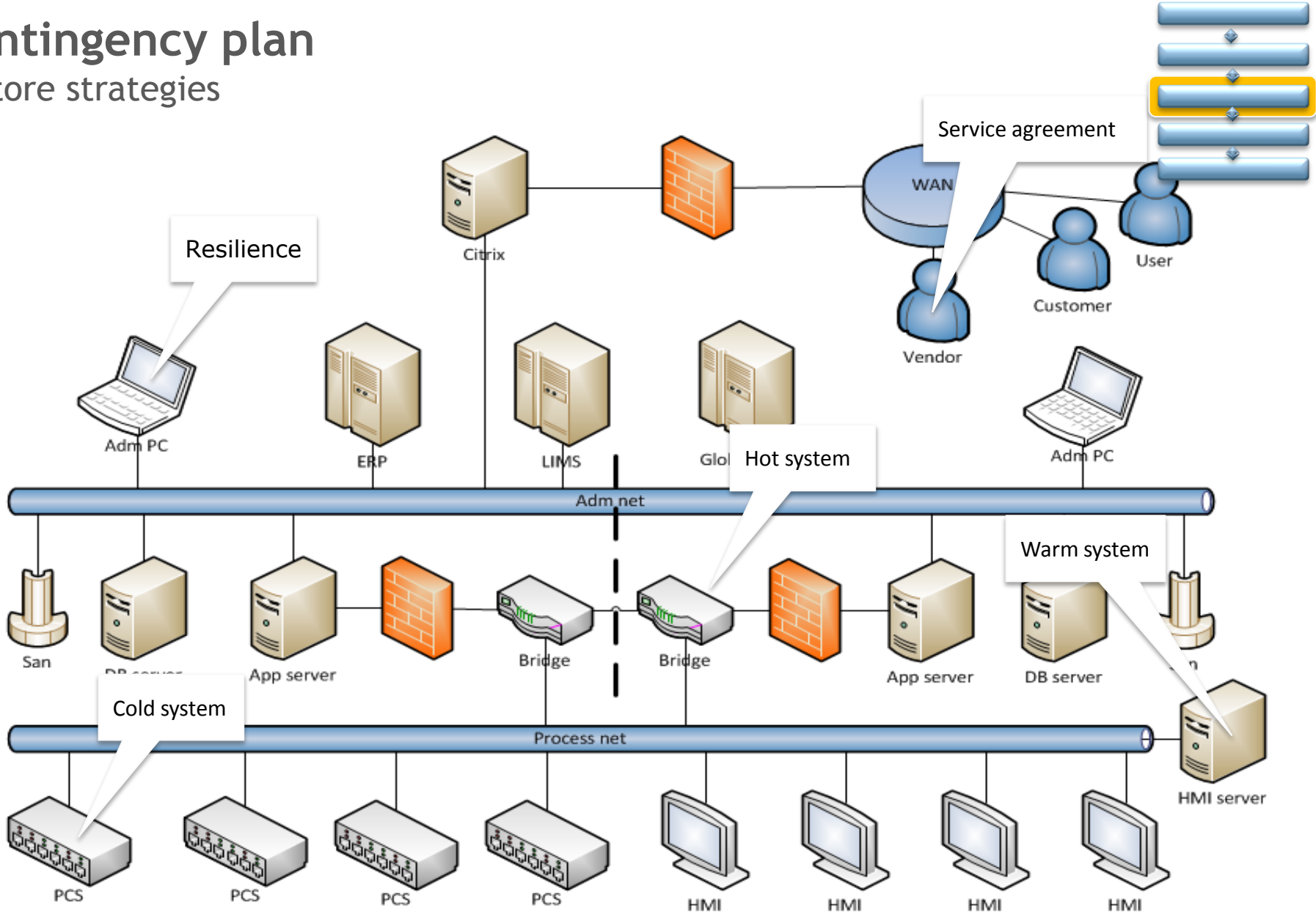
Service documentation

- Known error database
- IT continuity plan
- Backup/recover procedure



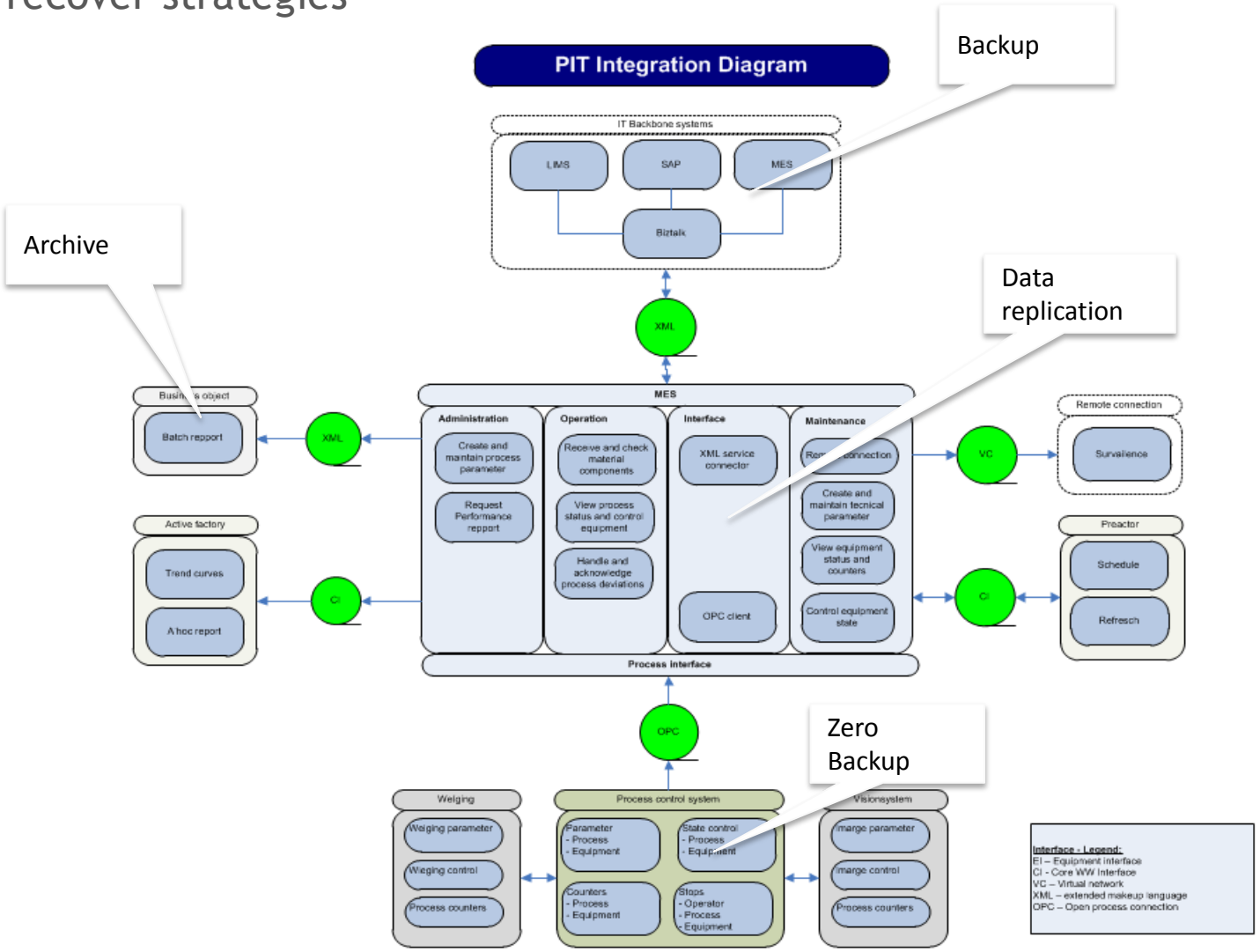
Contingency plan

Restore strategies



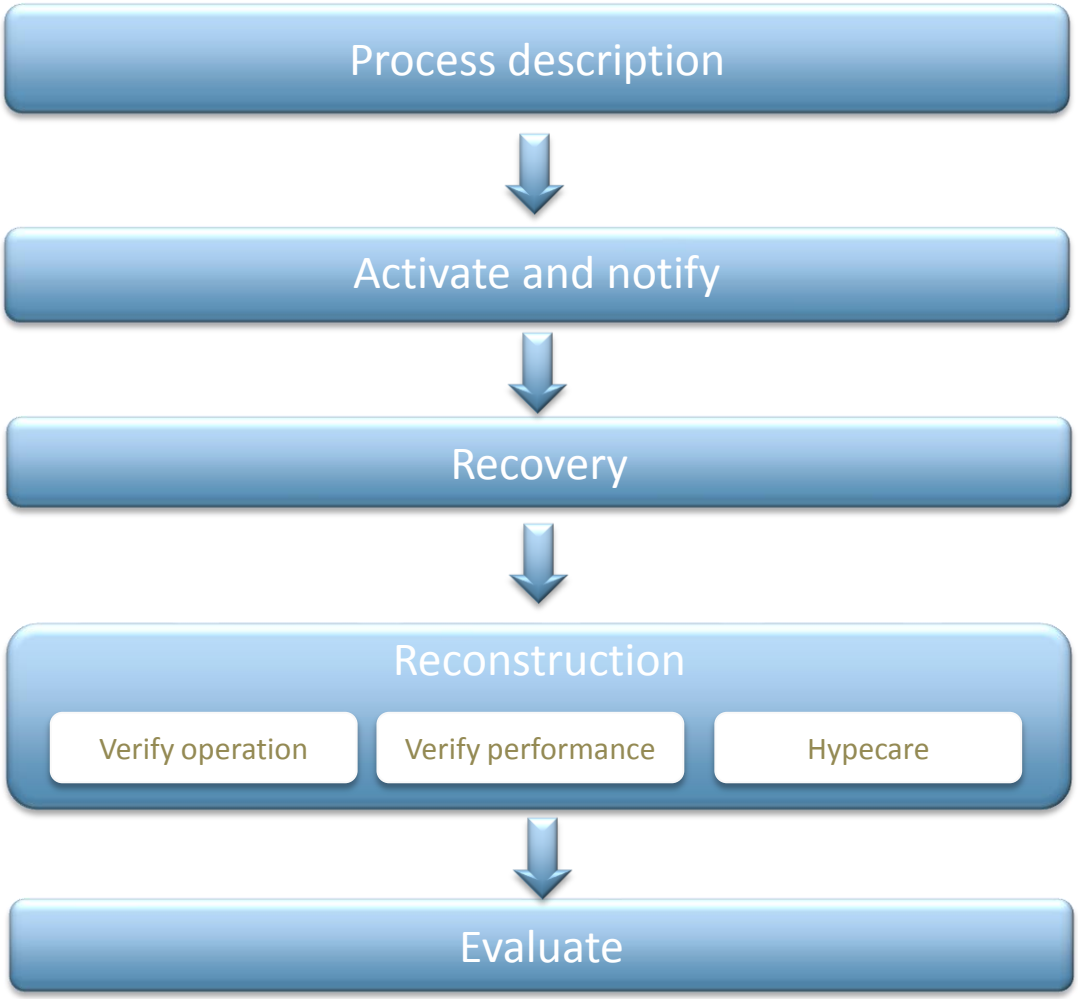
Contingency plan

Data recover strategies



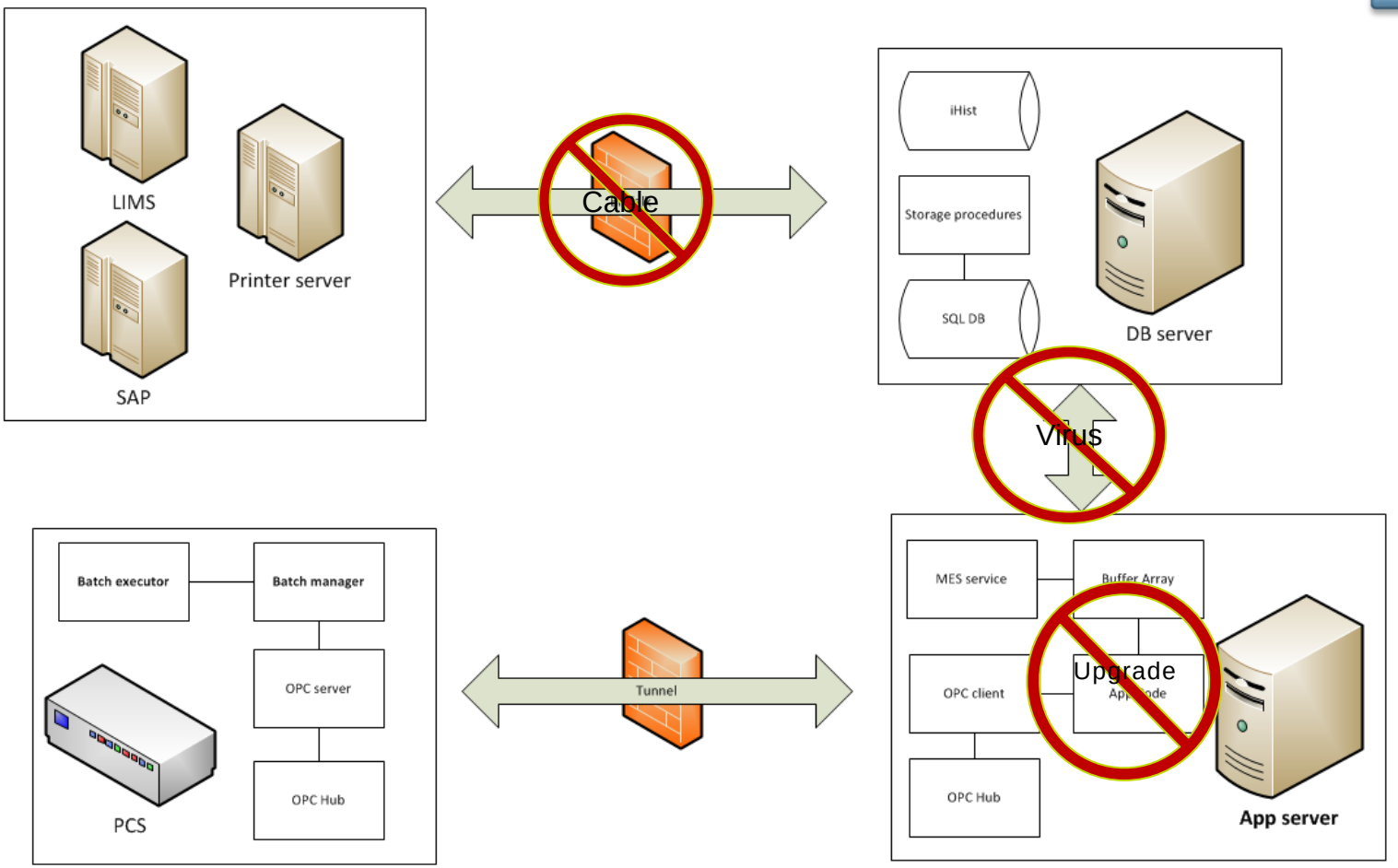
Contingency plan

Reconstruction



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

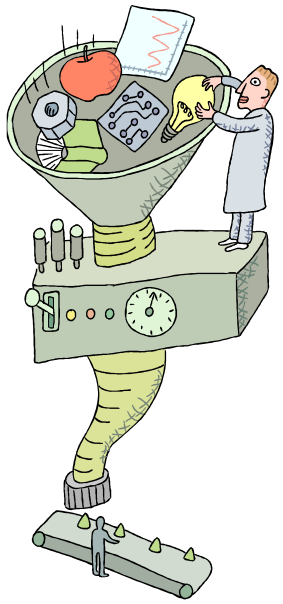
- Isolate process net
- Close down process computers and remove virus manually
- Install new windows path
- Develop and install a new virus cure

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

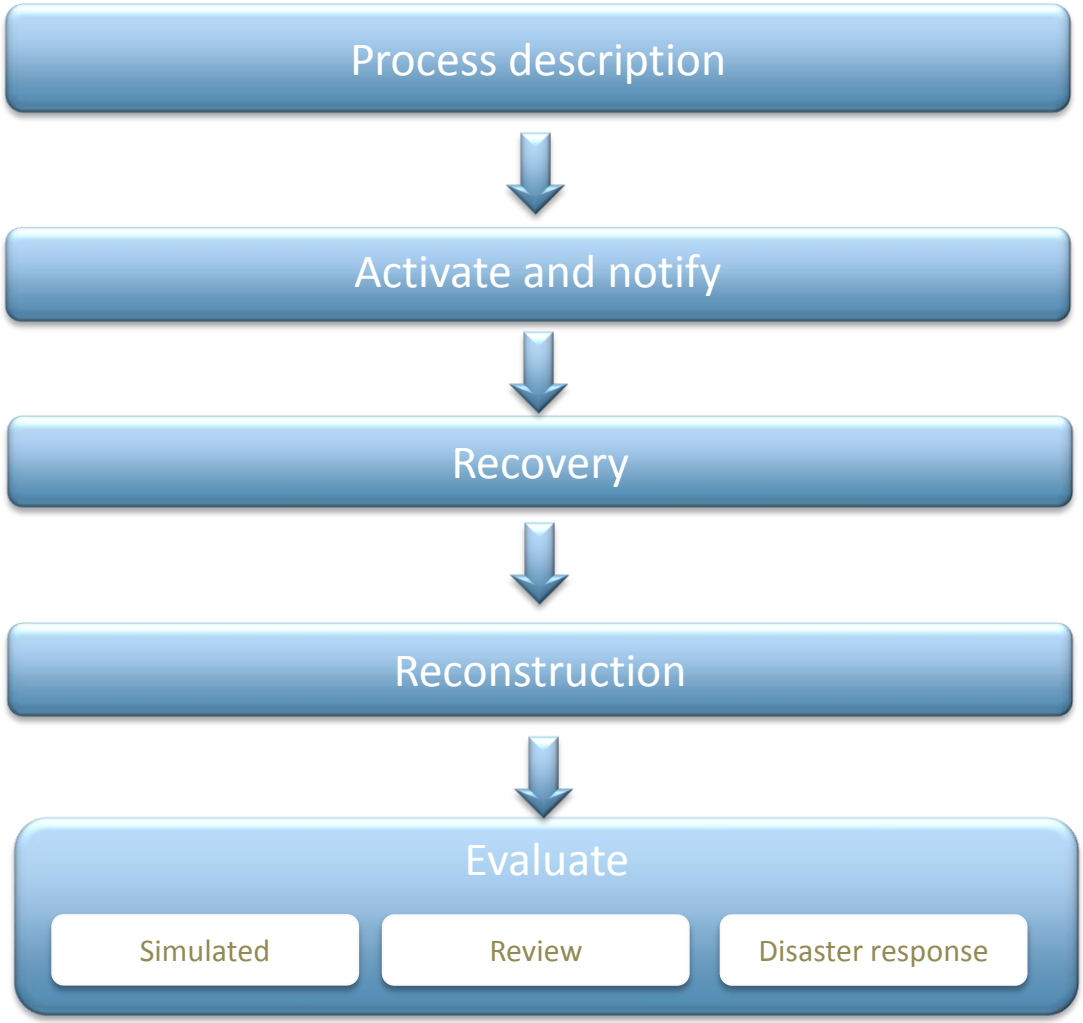
- Order parameter has to be typed in manually
- Performance information has to be log manually
- Information has to reviewed by another before use
- Temporary cable repair was conducted

Evaluation

Establish redundant server room with separated fiber and switch

Contingency plan

Evaluate



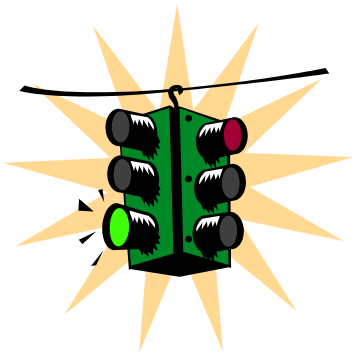
Contingency plan

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

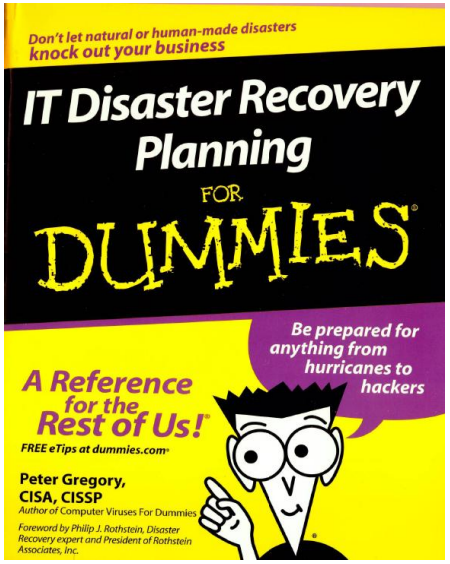
Definition and Abbreviations

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

CHR. HANSEN

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