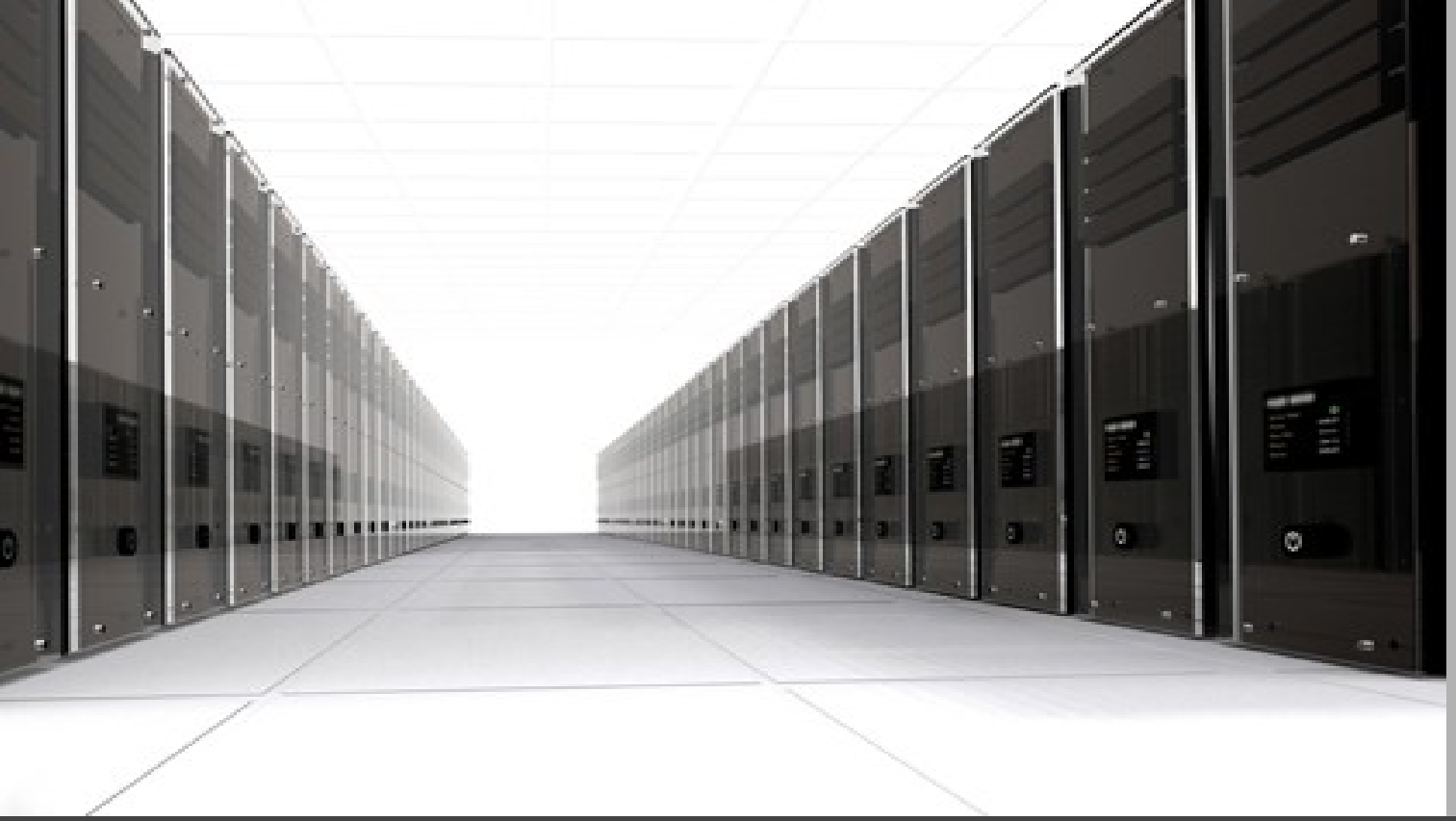


ICT READINESS FOR BUSINESS CONTINUITY

David López
(i Josep Ll. Berral)
V.1.1
Spring 2025

UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

General organizations:

Governance – **Management** - **Execution**

Automation: This is about automating **tasks**

Orchestration: This is about automating **processes**

Monitoring: You need good, trustful and up-to-date information to take decisions

KPI (Key Performance Indicators): in IT they are indicators of how are we achieving our goals

BIA: Business Impact Analysis

RA: Risk Analysis. What could possibly go wrong?

RTO: Recovery Time Objective

RPO: Recovery Point Objective

Fault & Error (I)

Fault: some problem (hardware, software, bugs, cyberattack)

Error: unnoticed problem or an impossible to recover error

- Server with ECC RAM detects erroneous bit and corrects it before sending it to CPU
- Server with ECC RAM detects several erroneous bits and cannot correct them before serving the CPU
- Server without ECC RAM has an erroneous bit and the CPU reads it
- An Ethernet data packet has been received and an erroneous bit has been detected
- A magnetic disk cannot read a data block
- A ransomware attack took place and data has been encrypted

Faults are inevitable

A company application cannot accept errors, so a company requires:

- **FT (Fault Tolerance):** Ability to continue to function error-free despite existing faults
- **HA (High Availability):** Ability to not stop services even with a large number of faults
- **DR (Disaster Recovery):** Ability to maintain service and not lose data even in large-scale disasters

SLA (Service Level Agreement): Defines policy in FT, HA and DR

Strategies. Schemes to achieve FT, HA and DR characteristics in a design (e.g. geographic dispersion, redundancy). They are abstractions

Technology. Concrete solutions to implement strategies (RAID, Distributed File Systems, Copy-on-Write are three technologies that offer disk fault-tolerancy)

ISO/IEC 27031:2011

- Encompasses all events and incidents (including security related) that could have an impact on ICT infrastructure and systems.
- It includes and extends the practices of information security incident handling and management and ICT readiness planning and services.
- IRBC (ICT Readiness for Business Continuity): a management system oriented to disaster recovery based on the Plan-Do-Check-Act model
- Part of ISO/IEC 27000 series https://en.wikipedia.org/wiki/ISO/IEC_27000-series

Disaster Recovery

iso.org/standard/44374.html

Meet Classes DAv... | UPClink | EduSTEAM | eBIB | Google Acadèmic | DeepL | Vacaciones | CODDI | Varios | Traductor de Goo... | Otros marcadores

ISO | Standards | About us | News | Taking part | **Store** | Search

This standard was last reviewed and confirmed in 2020. Therefore this version remains current.

Abstract

Preview

ISO/IEC 27031:2011 describes the concepts and principles of information and comunication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity. It applies to any organization (private, governmental, and non-governmental, irrespective of size) developing its ICT readiness for business continuity program (IRBC), and requiring its ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents, and related disruptions, that could affect continuity (including security) of critical business functions. It also enables an organization to measure performance parameters that correlate to its IRBC in a consistent and recognized manner.

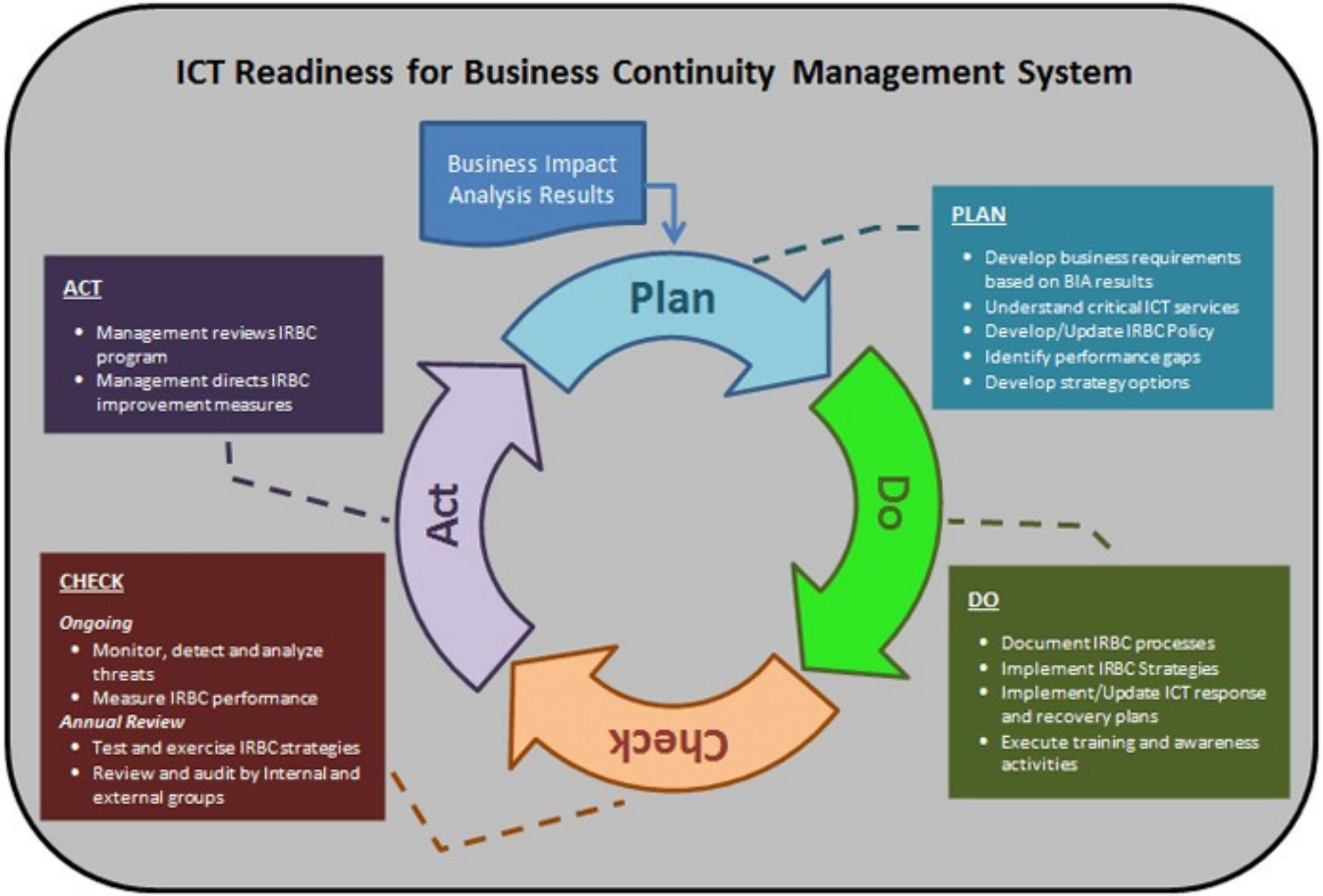
The scope of ISO/IEC 27031:2011 encompasses all events and incidents

Buy this standard

Format	Language
✓ PDF	English
Paper	English

CHF 166

Buy

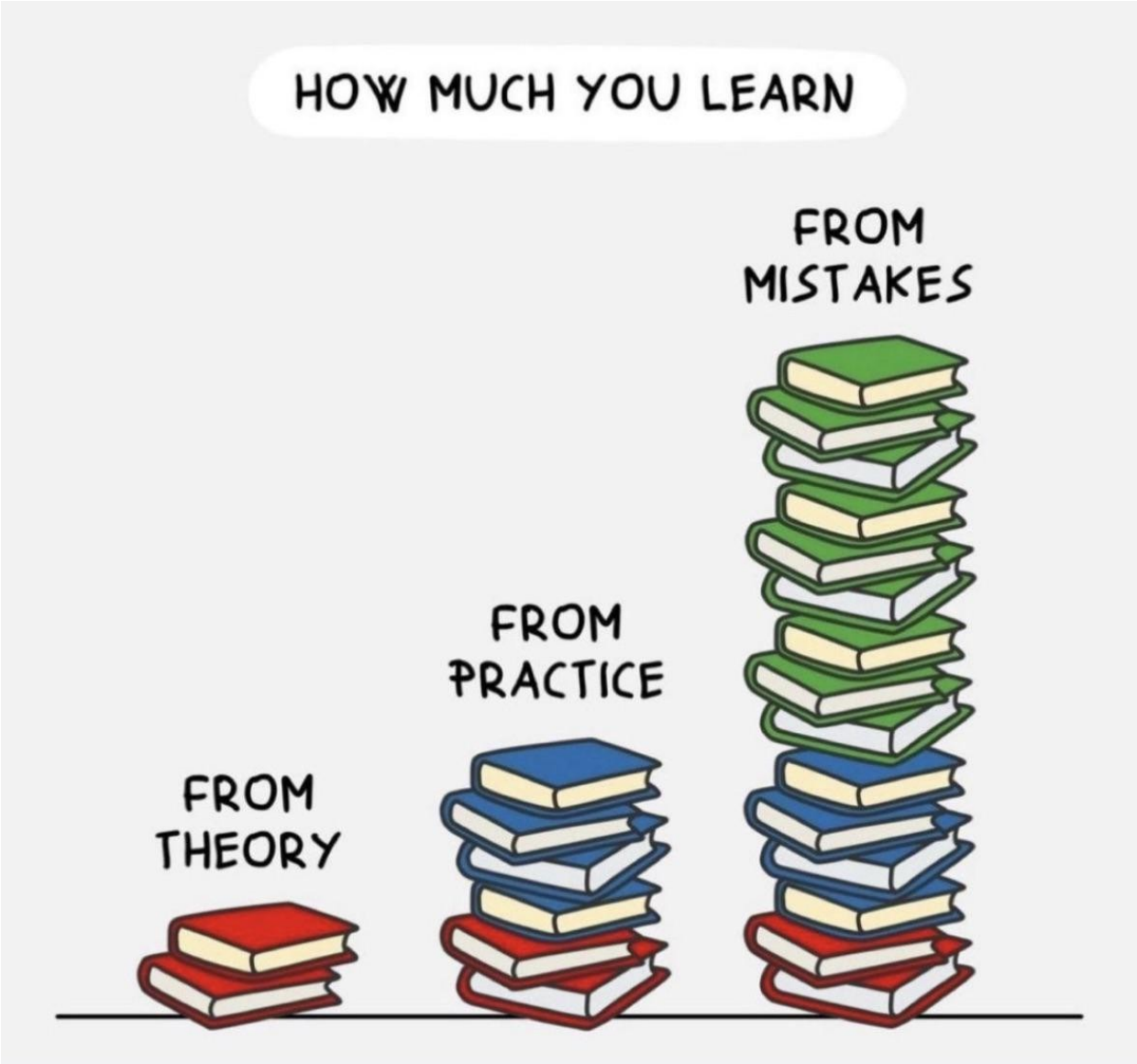

ICT Readiness for Business Continuity Management System
Business Impact Analysis Results
Plan
Do
Check
Act
PLAN
Develop business requirements based on BIA results
Understand critical ICT services
Develop/Update IRBC Policy
Identify performance gaps
Develop strategy options
DO
Document IRBC processes
Implement IRBC Strategies
Implement/Update ICT response and recovery plans
Execute training and awareness activities
CHECK
Ongoing
Monitor, detect and analyze threats
Measure IRBC performance
Annual Review
Test and exercise IRBC strategies
Review and audit by Internal and external groups
ACT
Management reviews IRBC program
Management directs IRBC improvement measures

Plan-Do-Check-Act

Plan	Establish IRBC policy, objectives, targets, processes and procedures relevant to managing risk and improving ICT readiness to deliver results in accordance with an organization's overall business continuity policies and objectives.
Do	Implement and operate the IRBC policy, controls, processes and procedures (automation and orchestration).
Check	Assess and, where applicable, measure process performance against IRBC policy, objectives and practical experience, and report the results to management for review.
Act	Take corrective and preventive actions, based on the results of the management review, to achieve continual improvement of the IRBC.

Is this enough? NOPE!

TEST: based on objectives and KPIs



1.- Identify critical system (CIO)

Hospital. Programmed surgeries. Four applications involved

- Data Base of patients (history)
- BD operation room staff
- Operation room management
- Scheduling

1.- Identify critical system (CIO)

Hospital. Programmed surgeries. Four applications involved

- Data Base of patients (history)
- BD operation room staff
- Operation room management
- Scheduling

2.- Define RPO/ RTO (CEO+CIO)

- 1 hour / 2 hour

1.- Identify critical system (CIO)

Hospital. Programmed surgeries. Four applications involved

- Data Base of patients (history)
- BD operation room staff
- Operation room management
- Scheduling

2.- Define RPO/ RTO (CEO+CIO)

- 1 hour / 2 hour

3.- Identify possible threats (CIO+CTO)

- A physical server crashes
- One disc of the server fails
- The whole disk server crashes
- A ransomware attack

4.- Prevention strategy (includes technology CIO – CTO - CISO)

- OSSIM software (and other malware systems) / Cybersecurity team
- Monitoring (disk odd access pattern)
- Frequent backups disconnected from the system
- Educating employees (IT & not IT)
- Maintain OS and other software up to date
- Hardware and software inventory need for a response
  - Critical / Important / Unimportant
- Identify personnel roles
  - Responsibility for: 1) declaring a disaster, 2) managing the crisis and recovering from it, 3) contacting third-party vendors, 4) reporting to management and liaising with customers, press

All this must be described and documented

5.- Response strategy

- Stop writes in discs
- Interrupt any ongoing backup
- Shutdown servers
- Notify people in charge
- …

6.- Response action steps

- Step by step (automated and manual)
- Boot every server, testing if everything is OK (search for malware, reinstall some software, …)
- Test access to data
- …
- All these procedures tested and audited
- All IT staff must have a complete knowledge of the procedures

Yes, it was a ransomware attack

7.- Recovery strategy

- Start servers in other location / Launch normal servers
- Detect lost data
- Assure system is safe
- A clear procedure to continue business with minimum required data in RTO
- …

8.- Recovery action steps

- Step by step (automated and manual)
- Inform stakeholders and clients ASAP
- Start with critical hard, soft & data, and continue to fully recovery
- …
- All these procedures tested and audited
- Staff in charge of recovery

Example

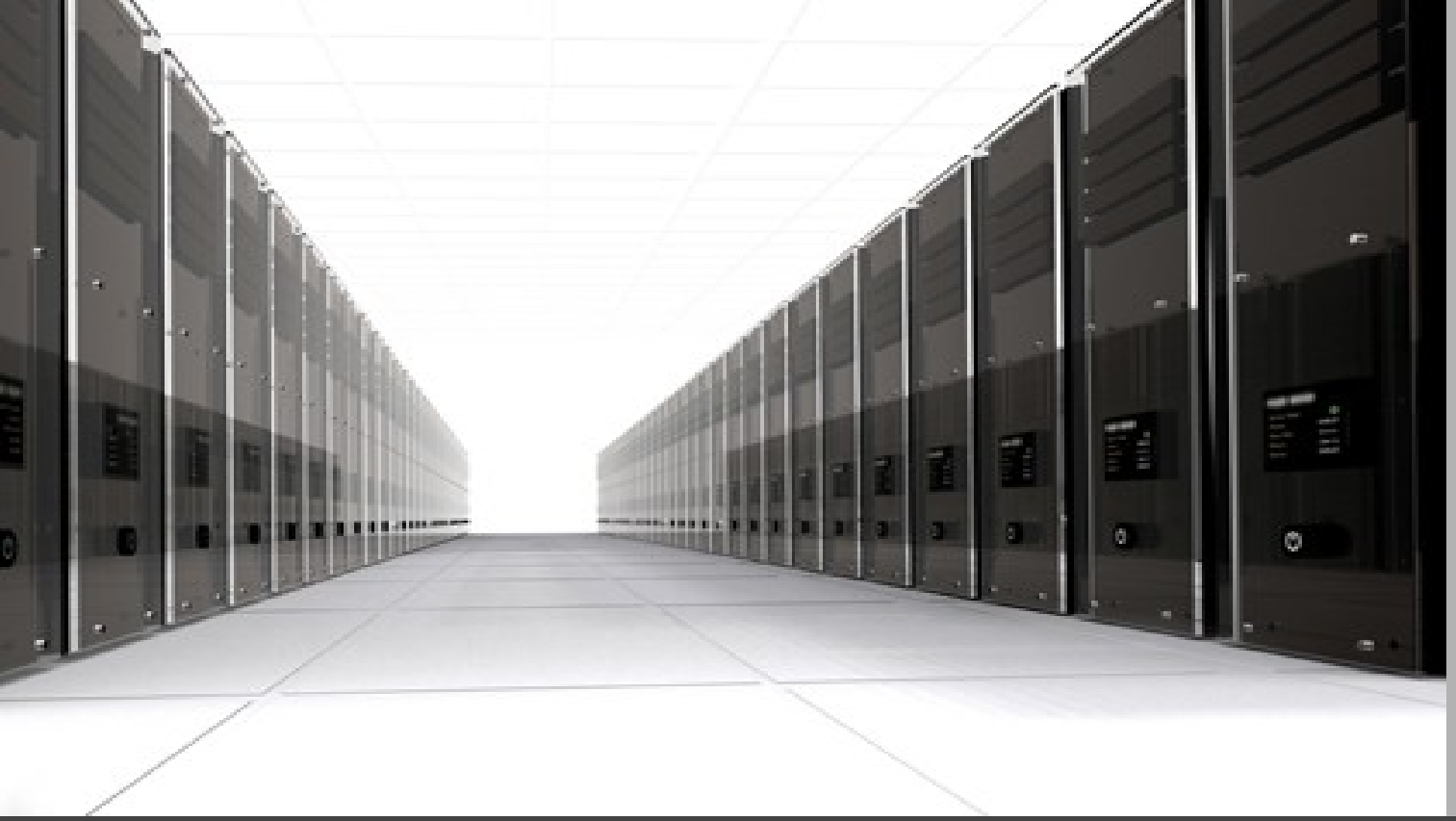
1.- Identify critical system
2.- Define RPO/ RTO
3.- Identify possible threats
4.- Prevention strategy
5.- Response strategy
6.- Response action steps
7.- Recovery strategy
8.- Recovery action steps

Example

1.- Identify critical system
2.- Define RPO/ RTO
3.- Identify possible threats
4.- Prevention strategy
5.- Response strategy
6.- Response action steps
7.- Recovery strategy
8.- Recovery action steps

- A university
- Sales company (Desigual, El Corte Inglés, FNAC, …)
- A streaming service (Netflix,…)
- Some public service (TMB, for instance)

Groups and work on



ICT READINESS FOR BUSINESS CONTINUITY

David López
(i Josep Ll. Berral)

UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH