FUJITSU

Secure the Continuity of IT Services and Business

Prepare, Protectand Recover

TiVi Data Center & Cloud 2025

February 6, 2025

Vesa-Matti Lindström

FUJITSU-PUBLIC





Vesa-Matti Lindström

Head of Hybrid IT Portfolio

Fujitsu Finland Hybrid IT – Portfolio & Product Management

Contact details



+358 40 920 2699



Vesa-matti.lindstrom@fujitsu.com



Helsinki, Finland



Areas of responsibility

- Head of Hybrid IT –Portfolio
- Head of Portfolio & Product Management Team
- Strategy & Vision of our Portfolio
- Product & Service
 Development Lead

Professional journey

- +15 years of experience in IT and Telecom business
- From sales, to business development, and portfolio leadership

Outside of work

- Family with 5-year-old son, wife, dog
- Family time, snowboarding, disc golf, bouldering

Key topics

Current operating environment in which organizations need to navigate in

The role of Business Continuity Plan in safe-guarding the infrastructure and business.

What needs to be addressed in the Business Continuity Planning?

Possible future threats for the business and infrastructure continuity

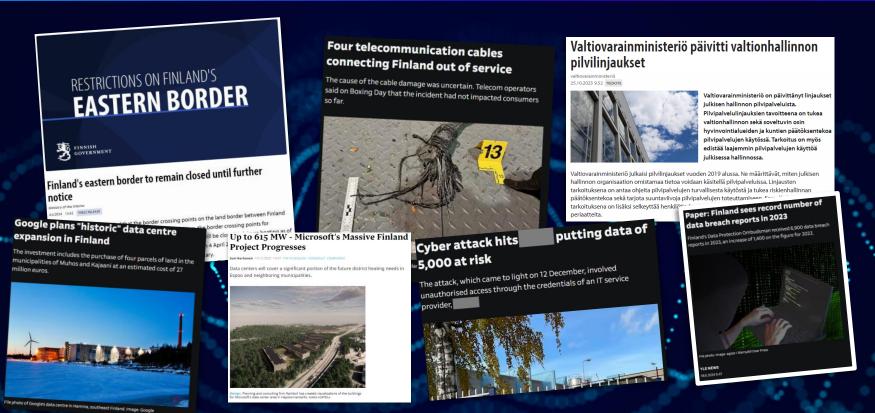
Takeaways

How to prepare for possible events and disasters. How to implement Business continuity. What kind of strategic choices we can encounter



What kind of status-quo and operating environment are we in?





How to ensure infrastructure and service continuity in today's challenging operational environment



Technologies and technical solutions can take you far, but not all the way. It's even more about making strategic choices and decisions, than just pure technology.

In order to ensure comprehensive Business Continuity, you need to have a plan.

Key elements for fundamental Business Continuity planning:

- 1. Business Impact Analysis (BCI)
- 2. Risk assessment and vulnerability analysis
- 3. Implementing redundant and resilient infrastructure
- 4. Crisis management and communication strategies
- 5. Regular testing, updates, and continuous improvement

Business Impact Analysis (BIA)



Business Impact Analysis (BIA)

Risk assessment and vulnerability analysis

Implementing redundant and resilient infrastructure

Crisis management and communication strategies

Regular testing, updates, and continuous improvement

BIA is the process of analyzing the impact over time of a disruption on the organization.

- 1. Identify Critical Business Functions
- 2. Assess Potential Impacts
- 3. Determine Recovery Time Objectives (RTO) & Recovery Point Objectives (RPO)
- 4. Prioritize Recovery Efforts
- 5. Develop Risk Mitigation Strategies

- Maximum tolerable period of disruption (MTPD)
- Minimum business continuity objective (MBCO)
- Recovery point objective (RPO)
- Recovery time objective (RTO)

Risk assessment and vulnerability analysis



Business Impact Analysis (BIA)

Risk assessment and vulnerability analysis

Implementing redundant and resilient infrastructure

Crisis management and communication strategies

Regular testing, updates, and continuous improvement

You can make the assessment and analysis yourself, order it, or utilize existing material. The most important thing is, that is suits your needs, organization, and operational environment.

If you choose to do it yourself, consider at least these:

- Define business continuity and infrastructure resilience
 - What they mean to you?
- Discuss methods for assessing vulnerabilities and their potential impact.
- Identify potential risks to infrastructure and business processes.

Implementing redundant and resilient infrastructure



Business Impact Analysis (BIA)

Risk assessment and vulnerability analysis

Implementing redundant and resilient infrastructure

Crisis management and communication strategies

Regular testing, updates, and continuous improvement

- The role of redundancy in critical systems (e.g., data centers, networks).
- Leveraging cloud services and backup solutions for resilience.
- Implement redundancy in all levels.
- How to do it? Yourself or utilizing partners
- Require Business Continuity Framework from your partners and build it together.
- Are the Backup systems applicable?
- Are the Disaster recovery systems and processes functional?

Crisis management and communication strategies



Business Impact Analysis (BIA)

Risk assessment and vulnerability analysis

Implementing redundant and resilient infrastructure

Crisis management and communication strategies

Regular testing, updates, and continuous improvement

In case of event, everyone needs to know what to do. Effective communication minimizes panic, misinformation, and operational disruptions.

When building your Crisis Management and Communications plans, consider these:

Communication Strategy

- Crisis Communication Plan
- Stakeholder Mapping
- Communication Channels & Redundancy
- Spokesperson & Media Management
- Real-Time Monitoring & Feedback Loop
- Training & Simulation Exercises

Crisis management

- Crisis Response Plan
- Incident Command Structure (ICS)
- Emergency Response Procedures
- Resource Allocation & Logistics
- Compliance & Regulatory Requirements

Regular testing, updates, and continuous improvement



Business Impact Analysis (BIA)

Risk assessment and vulnerability analysis

Implementing redundant and resilient infrastructure

Crisis management and communication strategies

Regular testing, updates, and continuous improvement

- It is important to test the BCP through simulations and drills.
- Adapt to new threats and evolving technologies through regular BCP updates.
- Require participation from partners.

Possible future threats and risks



- The evolution of Al
- High Performance Computing and Quantum Computing
- The development of geopolitical circumstances
- Climate change and environmental risks
- Regulations, legislation, and compliance
- Future energy supply and evolution of energy industry
- Supply chain vulnerability

Summary and key takeaways



- It's not rocket science; prepare and execute, and develop consistently.
- You don't have to do everything yourself, benefit from your partners.
- Utilize technology.
- Prepare for the worst, rather than be too optimistic.
- Prepare for the future.





