

Business Continuity Planning

Marcus Bendtsen

Institutionen för Datavetenskap (IDA)

Avdelningen för Databas- och Informationsteknik (ADIT)

Business Continuity Planning (BCP)

- Disasters eventually strike every organisation:
 - **Natural disasters:** Hurricanes, earthquakes, epidemics, etc.
 - **Man-made:** Building fire, burst water pipes, sabotage, piracy, etc.
- Disasters can threaten the operations of an organisation or even their very existence.



Business Continuity Planning (BCP)

- Business continuity seems intuitive.
- We should take measures to ensure that the company is not wiped out.
- What if Google did not have a business continuity plan?
- What if a rare, but still possible, storm hit Google's servers and destroyed all of them?

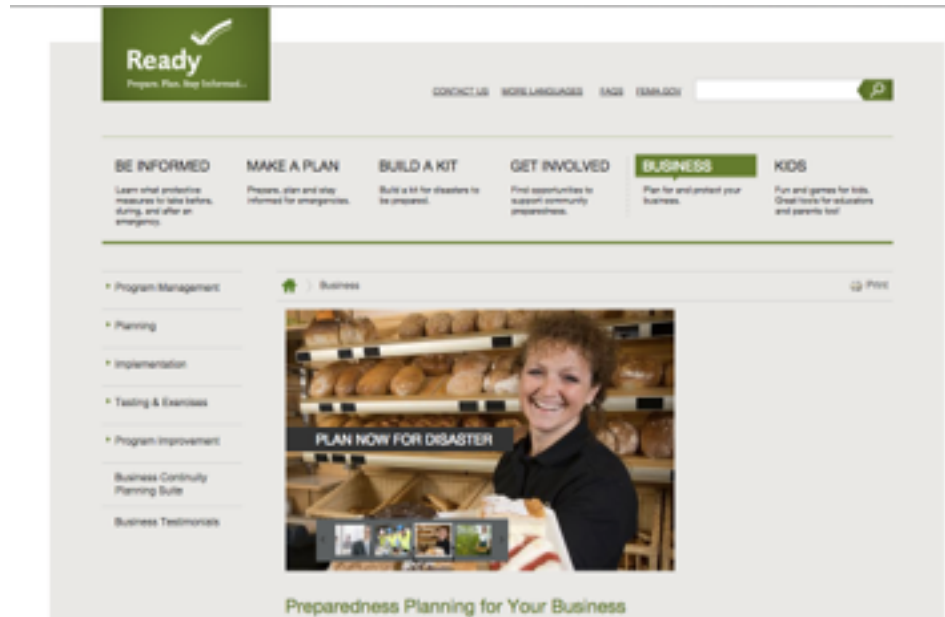


Business Continuity Planning (BCP)

- Resilient organisations have plans and procedures in place to mitigate the effects of a disaster on their operations and to help speed the return to normal operation.
- Business Continuity Planning (BCP):
 - **Assess** the risks to organisational processes.
 - Create **policies**, **plans** and **procedures** to minimise the impact those risks might have on the organisation, if they were to occur.
 - The goal of BCP planners is to ensure that the impact of disruptive events on the business is as small as possible.

Business Continuity Planning (BCP)

- 2004 – Department of Homeland Security launched *Ready* business which encourages small- to mid-sized businesses to create a BCP plan.
- www.ready.gov/business
- Detailed instructions and documents that help to create, test and maintain continuity plans.



Business Continuity Planning (BCP)

- BCP focuses on maintaining operations with ***reduced*** or ***restricted*** capabilities or resources.
- **As long as the mission-critical tasks of the organisation are maintained**, the BCP can be used.
- If the mission-critical tasks can not be performed, then the organisation is in *disaster mode*.
- Once in disaster mode, the ***disaster recovery planning*** takes over.

Business Continuity Planning (BCP)

Example

- Assume you are in charge of BCP at a company.
- You need the land-line phones to work in order for the mission-critical processes of your organisation to run.
- You are aware that sometimes the land-lines go down.
- Your solution to this is to have mobile phones ready-to-go that cover 80% of the employees.
- **Event:** Land-lines go down.
 - Your BCP kicks in, employees are given mobile phones, and mission-critical processes can continue – Your BCP is successful, and once land-lines are back, processes go back to normal.

Business Continuity Planning (BCP)

Example

- Assume you are in charge of BCP at a company.
- You need the land-line phones to work in order for the mission-critical processes of your organisation to run.
- You are aware that sometimes the land-lines go down.
- Your solution to this is to have mobile phones ready-to-go that cover 80% of the employees.
- **Event:** Complete power-outage, land-lines and mobile phone base stations are shut down.
- Your BCP is of no use now, instead the organisation is in *disaster mode* and ***disaster recovery planning*** should take over.

Business Continuity Planning (BCP)

Considerations

- But it is not only the state of the land-lines that determine if business can run:
 - Quality of land-lines in other countries (where the customers are).
 - Not being able to hire people for the call-centre.
 - Natural disasters preventing employees getting to work.
 - Strikes.
 - Servers going down.
 - etc.

Business Continuity Planning (BCP)

- Businesses vary greatly in geographical locations, mission-critical tasks, exposure, legal restrictions, etc.
- The agenda for this lecture is to give you an idea of what BCP is about, not to give you exact tasks that need to be completed in case of an event.
- The actual tasks that need to be done are dependent on the context and business needs.
- The next lecture will focus on disaster recovery and physical security, then we will look at more hands-on actions that can be used to protect the company.

The BCP process

- The BCP process has four steps:
 - **Project scope and planning**
 - Business impact assessment
 - Continuity planning
 - Approval and implementation
- We deal with this first* →

The BCP process



Project scope and planning

- Team members
 - The individual(s) **responsible** for the BPC process (*probably you*).
 - Representatives from each of the organisation's **departments responsible for core services** (e.g. call-centre department, marketing, sales).
 - Representatives from key **support departments** (e.g. in-house tech-support, human-resources).
 - IT representatives that have **expertise** in areas covered by BCP.
 - **Legal representatives** that are familiar with legal, regulatory, and contractual responsibilities.
 - Representatives from **senior management**.

The BCP process



Project scope and planning

- Team members
 - Individuals will have biases towards their expertise, e.g. representatives from operational departments will think that their department is most critical.

This is not necessarily a bad thing, if ***the leader is able to navigate*** and balance these biases then the BCP will cover all the organisations needs.

The BCP process



Project scope and planning

- Team members
 - Individuals will have biases towards their expertise, e.g. representatives from operational departments will think that their department is most critical.

No peacocks, jerks or whiners

- Timothy Geithner

The BCP process



Project scope and planning

- Resource requirements
 - **BCP Development**
 - The team you have gathered will require some resources to perform the four steps in the BCP process.
 - The main cost is the effort of the members.
 - Some members may not need to take part in every meeting, so scheduling members' time is important to estimate the cost of BCP.

The BCP process



Project scope and planning

- Resource requirements
 - **BCP Testing, Training and Maintenance**
 - Once the BCP process is complete it is important to test, train and maintain the process.
 - Will usually require some hardware and software commitments, but the biggest cost will be employees involved in the activities.
 - A plan that is not tested is more or less useless, so if the test costs are going to be very high then considerations needs to be made.

The BCP process



Project scope and planning

- Resource requirements

- **BCP Implementation**

- If the BCP needs to go into action, then a large amount of resources will go into the activities.
 - This may require significant hardware/software and employee costs.
 - Estimating these costs are hard, but a figure needs to be decided upon, spending millions of dollars to protect a business worth a fraction of this may not be feasible.

The BCP process



Project scope and planning

- Resource requirements
 - The BCP team should get preliminary approval of senior management for the resource required.
 - It helps to have senior management in the BCP team, as they can directly weigh-in on the resource requirements.
 - Continuing with the BCP process without having a preliminary O.K. that the resources will be available is futile, there is no point making plans if the plans can never be executed.

The BCP process



Project scope and planning

- Legal and Regulatory Requirements
 - Industries may be bound by laws and regulations that force the BCP to act in certain ways.
 - Banks may be under laws that force them to be able to cope with certain economical events.
 - Pharmaceutical companies that work in less-than-optimal circumstances may have to verify that the purity of their products have not changed.

The BCP process



Project scope and planning

- Legal and Regulatory Requirements
 - Many service companies operate under *service-level-agreements* (SLA) that can incur monetary penalties if they are breached.
 - Company A promises to deliver a service monthly to company B, if they miss a deadline then they must pay a fine to B according to a previously decided contract.

The BCP process



Project scope and planning

- Legal and Regulatory Requirements
 - Clauses in contracts that may mitigate the consequence of a risk.
 - In contracts between A and B it may state that deadlines are allowed to be missed in case there is a fire in the main office.

The BCP process

- The BCP process has four steps:
 - Project scope and planning
 - **Business impact assessment** ← *... moving on...*
 - Continuity planning
 - Approval and implementation

The BCP process



Business Impact Assessment (BIA)

- Much like risk analysis, BIA identifies resources that are critical to an organisation's mission-critical processes and the threats posed to those resources.
- Likelihood and impact of the threats are assessed.
- The analysis can be quantitative or qualitative, but usually is a combination of both.

The BCP process



Business Impact Assessment (BIA)

Requires good leadership!

- Identify priorities
 - Create a **list of business processes** and rank them in order of importance.
 - A simple way to do this is to ask each team member to come up with a list for their specific department/expertise.
 - Then the team merges these lists into a master list for the entire organisation.
 - Now you have a qualitative list of priorities.
 - This list is used as input to the BIA as a starting point.

The BCP process

List of process priorities as decided by the team members.

1. Call-centre operations
2. Sales and marketing
3. Recruitment
4.
5.
6.
7. Christmas party organisation

List of business processes

- Qualitative list of priorities.
- Used as input to the impact assessment.

The BCP process



Business Impact Assessment (BIA)

- Identify priorities
 - The list of priorities can be used to identify the **assets** of the organisation that are important to the prioritised operations.
 - The BCP team lists all of the organisations **assets**, and quantifies them in monetary terms, known as *asset value* (AV).

The BCP process

List of process priorities as decided by the team members.

1. Call-centre operations
2. Sales and marketing
3. Recruitment
4.
5.
6.
7. Christmas party organisation

Asset values (AV)

- Office building \$100 000
- Workstations \$200 000
- Database with client data \$4 000 000
-
-
-
- Coffee-machine \$5

The BCP process



Business Impact Assessment (BIA)

- Identify priorities
 - Each business **function** is given a *maximum tolerable downtime* (MTD). The MTD is the maximum length of time the business function can be inoperable without causing irreparable harm to the business.
 - Each business **function** is given a *recovery time objective* (RTO). The RTO is the amount of time in which you think you can feasibly **recover** the function in the event of a disruption.
 - One of the goals of BCP is to ensure that $RTO < MTD$ for critical functions.

The BCP process



Business Impact Assessment (BIA)

- Documents so far...

List of process priorities as decided by the team members.

1. Call-centre operations
2. Sales and marketing
3. Recruitment
4.
5.
6.
7. Christmas party organisation

Asset values (AV)

- Office building \$100 000
- Workstations \$200 000
- Database with client data \$4 000 000
-
-
-
- Coffee-machine \$5

Functions

- Calling in-and-out from call centre
MTD = 2 hours
RTO = 6 hours
- Database backups
MTD = 24 hours
RTO = 12 hours
- ...
- ...

The BCP process



Business Impact Assessment (BIA)

- Risk identification
 - Natural risks
 - Violent storms/hurricanes/tornadoes/blizzards
 - Earthquakes
 - Mudslides/avalanches
 - Volcanic eruptions
 - Meteorite showers, sun flares, ...
 - Man-made risks
 - Terrorist acts/wars/civil unrest
 - Theft/vandalism
 - Fires/explosions
 - Prolonged power outages
 - Building collapses

List all risks the team can think of, do not worry about the likelihood or consequence, just identify the risks.

The BCP process



Business Impact Assessment (BIA)

- Likelihood assessment
 - Calculate the likelihood of the risks using *annualised rate of occurrence* (ARO).
 - The ARO is the number of times a business expects to experience a given risk each year.
 - Each risk identified should be given an ARO:
 - Use corporate history, professional experience, meteorologists, seismologists, fire prevention professionals and other consultants as needed.
 - U.S. Geological Survey has an earthquake map, that is available free-of-charge. This map shows the ARO for earthquakes in various regions in the US.
 - There are other resources available, such as flood maps.

The BCP process

Impact assessment

Annualised rate of occurrence

- Fire (ARO = 1/10)
- Flood (ARO = 1/5)
- Power-surge (ARO = 10)

The BCP process



Business Impact Assessment (BIA)

- Impact Assessment
 - The identified risks carry different impact on the business.
 - A fire may cause 70% of a building to be damaged, whilst a flood may cause 30% of the building to be damaged.
 - The *exposure factor* (EF) is the amount of damage that the risk poses to the asset, given as a percentage of the value, i.e. the EF of our building to flooding is 30%.

The BCP process

Impact assessment

Annualised rate of occurrence

- Fire (ARO = 1/10)
- Flood (ARO = 1/5)
- Power-surge (ARO = 10)

Exposure factor

- Building - Fire (EF = 70%)
- Building - Flood (EF = 30%)
- Building – Power-surge (EF = 2%)
- Database servers – Fire (EF = 45%)
- Database servers – Flood (EF = 60%)
- Database servers – Power-surge (EF = 2%)

The BCP process



Business Impact Assessment (BIA)

- Impact Assessment
 - The *single loss expectancy* (SLE) is the monetary loss that is expected each time the risk materialises:
 - $SLE = AV \times EF$
 - If our building is worth \$100 000 (AV), and the EF of Building – Flood is 30% then the SLE of flooding would be \$30 000.

The BCP process

Impact assessment

Annualised rate of occurrence

- Fire (ARO = 1/10)
- Flood (ARO = 1/5)
- Power-surge (ARO = 10)

Exposure factor

- Building - Fire (EF = 70%)
- Building - Flood (EF = 30%)
- Building – Power-surge (EF = 2%)
- Database servers – Fire (EF = 45%)
- Database servers – Flood (EF = 60%)
- Database servers – Power-surge (EF = 2%)

Single loss expectancy (SLE = AV * EF)

- Building - Fire (SLE = \$100 000 * 70% = \$70 000)
- Building - Flood (SLE = \$100 000 * 30% = \$30 000)
- Building – Power-surge (SLE = \$100 00 * 2% = \$2 000)
- Database servers – Fire (SLE = \$4 000 000 * 45% = \$1 800 000)
- Database servers – Flood (SLE = \$4 000 000 * 60% = \$2 400 000)
- Database servers – Power-surge (SLE = \$4 000 000 * 2% = \$80 000)

The BCP process



Business Impact Assessment (BIA)

- Impact Assessment
 - The *annualised loss expectancy* (ALE) is the monetary loss the business expects as a result of the risk harming an asset over a year.
 - $ALE = \text{Single Loss Expectancy} \times \text{Annualised Rate of Occurrence}$
 - $ALE = SLE \times ARO$
 - SLE for Building – Flood is \$30 000 and a flooding is expected every 5 years:
 - $ALE = \$30\,000 \times 1/5 = \$6\,000$
 - The business can expect to loose \$6 000 each year due to flooding.

The BCP process

Impact assessment

Annualised rate of occurrence

- Fire (ARO = 1/10)
- Flood (ARO = 1/5)
- Power-surge (ARO = 1/10)

Exposure factor

- Building - Fire (EF = 70%)
- Building - Flood (EF = 30%)

Annualised loss expectancy (ALE = SLE * ARO):

- Building - Fire (ALE = \$70 000 * 1/10 = \$7 000)
- Building - Flood (ALE = \$30 000 * 1/5 = \$6 000)
- Building - Power-surge (ALE = \$2 000 * 10 = \$20 000)
- Database servers - Fire (ALE = \$1 800 000 * 1/10 = \$180 000)
- Database servers - Flood (ALE = \$2 400 000 * 1/5 = \$480 000)
- Database servers - Power-surge (ALE = \$80 000 * 10 = \$800 000)

Single loss expectancy (SLE)

- Building - Fire (SLE = \$4 000 000 * 45% = \$1 800 000)
- Building - Flood (SLE = \$4 000 000 * 60% = \$2 400 000)
- Building - Power-surge (SLE = \$4 000 000 * 2% = \$80 000)
- Database servers - Fire (SLE = \$4 000 000 * 45% = \$1 800 000)
- Database servers - Flood (SLE = \$4 000 000 * 60% = \$2 400 000)
- Database servers - Power-surge (SLE = \$4 000 000 * 2% = \$80 000)

The BCP process



Business Impact Assessment (BIA)

- Impact Assessment - Qualitative
 - The qualitative impact on operations also needs to be assessed, as sometimes there are hidden impacts that cannot be quantified so easily:
 - Reputation – Negative publicity
 - Social/ethical responsibilities towards the community
 - Loss of employees to other jobs after prolonged downtime
 - Loss of goodwill among client base

The BCP process



Business Impact Assessment (BIA)

- Documents so far...

Lists from before...

List of process priorities as decided by the team members.

Asset values (AV)

Functions (MTD,RTO)

Annualised loss expectancy (ALE = SLE * ARO):

- Building - Fire (ALE = \$70 000 * 1/10 = \$7 000)
- Building - Flood (ALE = \$30 000 * 1/5 = \$6 000)
- Building – Power-surge (ALE = \$2 000 * 10 = \$20 000)
- Database servers – Fire (ALE = \$1 800 000 * 1/10 = \$180 000)
- Database servers – Flood (ALE = \$2 400 000 * 1/5 = \$480 000)
- Database servers – Power-surge (ALE = \$80 000 * 10 = \$800 000)

Qualitative measures

- Fire in building – loss of reputation is too great to recover from.
- Not being able to get to fire-exits – Legal repercussions.
- ...
- ...

The BCP process



Business Impact Assessment (BIA)

- Resource prioritisation
 - The entire team needs to get involved in merging the lists.
 - Qualitative prioritisation of asset protection is done by sorting by ALE.
 - Qualitative prioritisation of functions are prioritising those functions where recovery time objective (RTO) > maximum tolerable downtime (MTD)
 - Then the quantitative assessments need to be added
 - A company specialising in fire prevention will prefer to lose more money from flooding than to see their building burnt down (as it will have massive impact on their credibility).

The BCP process



Business Impact Assessment (BIA)

- Resource prioritisation

Prioritised list

1. Calling-in-and-out from call centre
MTD = 2 hours
RTO = 6 hours
2. Database servers – Power-surge (\$800 000)
3. Not being able to get to fire-exits – Legal repercussions.
4. Database servers – Flood (\$480 000)
5. ...
6. ...
7. Coffee-machine \$0.001

How this merging is done is not well defined, this is why it is crucial to have **team members that come from every department**, so that they can weigh in on what is important, **including senior management**.

The BCP process

- The BCP process has four steps:
 - Project scope and planning
 - Business impact assessment
 - **Continuity planning** ← *... moving on...*
 - Approval and implementation

The BCP process



Continuity Planning

- Strategy development
 - It is **impossible** to take the entire list of priorities and implement provisions to ensure zero-downtime in the face of every possible risk.
 - One needs to look at the priority list and choose what can be ignored and what should be addressed.
 - During strategy development the BCP team **selects the risks that require mitigation and allocate resources** to them.

The BCP process



Business Impact Assessment (BIA)

- Resource prioritisation

Prioritised list

1. Calling-in-and-out from call centre
MTD = 2 hours
RTO = 6 hours
2. Database servers – Power-surge (\$800 000)
3. Not being able to get to fire-exits – Legal repercussions.
- ~~4. Database servers – Flood (\$400 000)~~
5. ...
6. ...
7. Coffee-machine \$0.001

} Ignored

The BCP process



Continuity Planning

- Provisions and Processes
 - The BCP team designs and allocates specific procedures and mechanisms that will mitigate risks deemed unacceptable.
- Three main areas of concern:
 - People
 - Buildings and Facilities
 - Infrastructure

The BCP process



Continuity Planning

- Provisions and Processes
 - People
 - People should be safe after an emergency, this should always be the first priority of the BCP plan.
 - Ensure that the people in the organisation have the resources they need to comply with the BCP plan as well as continue the work they are supposed to do.
 - If the BCP dictates that employees should stay at the workplace for prolonged time during an event, then arrangements must be made for shelter, food and water.
 - Plans should include what to stockpile and when and how to rotate the stockpile to prevent spoilage.

The BCP process



Continuity Planning

- Provisions and Processes
 - Buildings and Facilities
 - The continuity plan should address two areas when it comes to facilities (such as office buildings, storage areas, depots, etc.).
 - **Hardening provisions:** BPC should outline mechanisms and procedures that can be put in place to protect existing facilities against risks defined in the strategy.
 - Fix leaky roof, install reinforced hurricane shutters, fireproof walls, install escape ladders, sprinkler systems, etc.
 - **Alternative sites:** More about this in *disaster recovery planning*.

The BCP process



Continuity Planning

- Provisions and Processes
 - Infrastructure
 - Computer systems that process orders, manages supply chains, handle customer service, allow for communication etc.
 - Servers, workstations, etc.
 - Two main methods of providing protection:
 - **Physically hardening systems** – Introduce computer-safe water suppression, install uninterruptible power supplies. More about this during *physical security*.
 - **Alternative systems** - More about this during *disaster recovery planning*.

The BCP process



Business Impact Assessment (BIA)

- Resource prioritisation

Prioritised list

1. Calling-in-and-out from call centre
MTD = 2 hours
RTO = 6 hours
2. Database servers – Power-surge (\$800 000)
3. Not being able to get to fire-exits – Legal repercussions.
4. Database servers – Flood (\$400 000)
5. Fire in building – loss of reputation is too great to recover from.
6. ...
7. ...
8. Coffee-machine \$0.001

Procedures and mechanisms (Plan)

1. Keep mobile phones ready, new RTO (recovery time objective) = 30 minutes.
2. Install surge protectors to decrease EF (exposure factor).
3. Install more signs pointing to fire exits and clear paths leading to them.

The BCP process

- The BCP process has four steps:
 - Project scope and planning
 - Business impact assessment
 - Continuity planning
 - **Approval and implementation** ← *... moving on...*

The BCP process

Approval and implementation

- Plan approval
 - This can be easy or difficult depending on how much senior management has been part of the process.
- Plan implementation
 - Once the plan has been approved it should be implemented.
 - A schedule for when and how the implementation should be done is useful.
 - Not all mechanisms can be implemented at the same time.



The BCP process



Approval and implementation

- Training and Education
 - All personnel who will be involved in the plan should receive training on the overall plan and individual responsibilities.
 - People with direct BCP responsibilities should have a backup person trained to ensure redundancy if the primary person is injured or cannot reach the workplace.

The BCP process



Approval and implementation


- Documentation
 - Solidifies what the plan is and what has been agreed upon.
 - The exact details are outside the scope of this introduction, but it includes:
 - Goals (What are the goals of the plan)
 - Importance (Senior executive should state the importance of the document)
 - Priorities, organisational responsibilities, urgency and timing, emergency-response guidelines
- Testing and exercise – Instructions on how to run exercises and train new employees should also be documented.

The BCP process



Approval and implementation

- Maintenance
 - The BCP team does not disband once the process is complete.
 - Every organisation changes, and the team should have regular meetings discussing any changes in priorities.
 - Small changes can be done as amendments to existing plans, but large changes may require the entire process to be redone.



Resiliency Services

Resiliency Assessment

Improve business continuity and resiliency by identifying and mitigating your availability risks

Achieving business continuity is critical to your organization's success. But how do you know you are investing in the right set of capabilities to develop a successful resiliency program targeted to your specific business requirements? IBM business continuity assessment offerings help you identify and evaluate potential risks and disruptions so you can understand their impacts on your current business environment. Using our custom-developed frameworks, blueprints, and models, our business continuity assessment experts recommend an improvement plan that encompasses crisis management and disaster recovery and is tailored to your needs.

Services we offer

Business impact analysis

Identify the most critical processes and functions for your business and the tangible and intangible impacts of a disruption, including potential cost of downtime. Our experienced consultants help you define your recovery objectives and resource dependencies so you better understand the value of business continuity planning. Our business impact analysis services create a foundation to help you plan your business continuity strategy and identify the best solutions to support it.

 [Download the fact sheet](#) (132KB)

 [Explore the benefits of Business Impact Analysis](#)

Recoverability assessment

Evaluate your IT disaster recovery and business continuity processes and discover how they stack up against your recovery objectives. Identify vulnerabilities preventing you from meeting your organization's business continuity goals. IBM recoverability assessment services can help identify specific requirements needed to recover from virtually any business disruption and define steps for resuming operations quickly and accurately.

 [Download the fact sheet](#) (133KB)

Resilience program assessment

Measure and compare the maturity of your resilience program against best practices and gain recommendations to move your strategy forward. IBM resilience program assessment services is customized to your specific business and industry needs and covers key areas including plans and procedures for business continuity, crisis management, disaster recovery, work area recovery, and IT and business programs.

 [Download the fact sheet](#) (119KB)

Risk assessment

Recognize and evaluate natural, physical, and social risks to your business operations. IBM risk assessment services help you pinpoint where your business is most vulnerable, identifying potential impacts and evaluating safeguards. We develop documented, customized recommendations to help you prioritize your assets and build a strong business case for investing in mitigation technologies and techniques.

 [Download the fact sheet](#) (119KB)

Availability assessment

Analyze your current strategy, organization, processes, applications, data, technology, and facilities to identify gaps in your business continuity plans. IBM availability assessment services take a methodology-driven approach to help you analyze the root causes of outages, the robustness of your IT availability architecture, and the strength of your supporting availability management processes. We then provide prioritized recommendations based on industry-leading practices.

 [Download the fact sheet](#) (134KB)

Business impact analysis features

IBM consultants are skilled at discovering key linkages between business priorities and IT policies and plans. Our experts have the extensive experience and methodologies needed to perform detailed inventories of your vital assets and processes. IBM's business impact analysis can:

- ✓ **Prioritize critical systems**

Identify which business processes and assets should be recovered first

- ✓ **Highlight interdependencies**

Map connections to understand how an outage of one system can affect others

- ✓ **Recommend recovery options**

Determine primary and alternative strategies for getting up and running

- ✓ **Detail recovery requirements**

Help you understand estimated recovery times and processes

- ✓ **Assess risk**

Examine the financial, productivity, and personal impact of a business disruption

- ✓ **Build a business case**

Provide financial data to help you justify business continuity investment

Is there a better plan?

Plan beats no plan

- Timothy Geithner



Linköpings universitet
expanding reality

www.liu.se