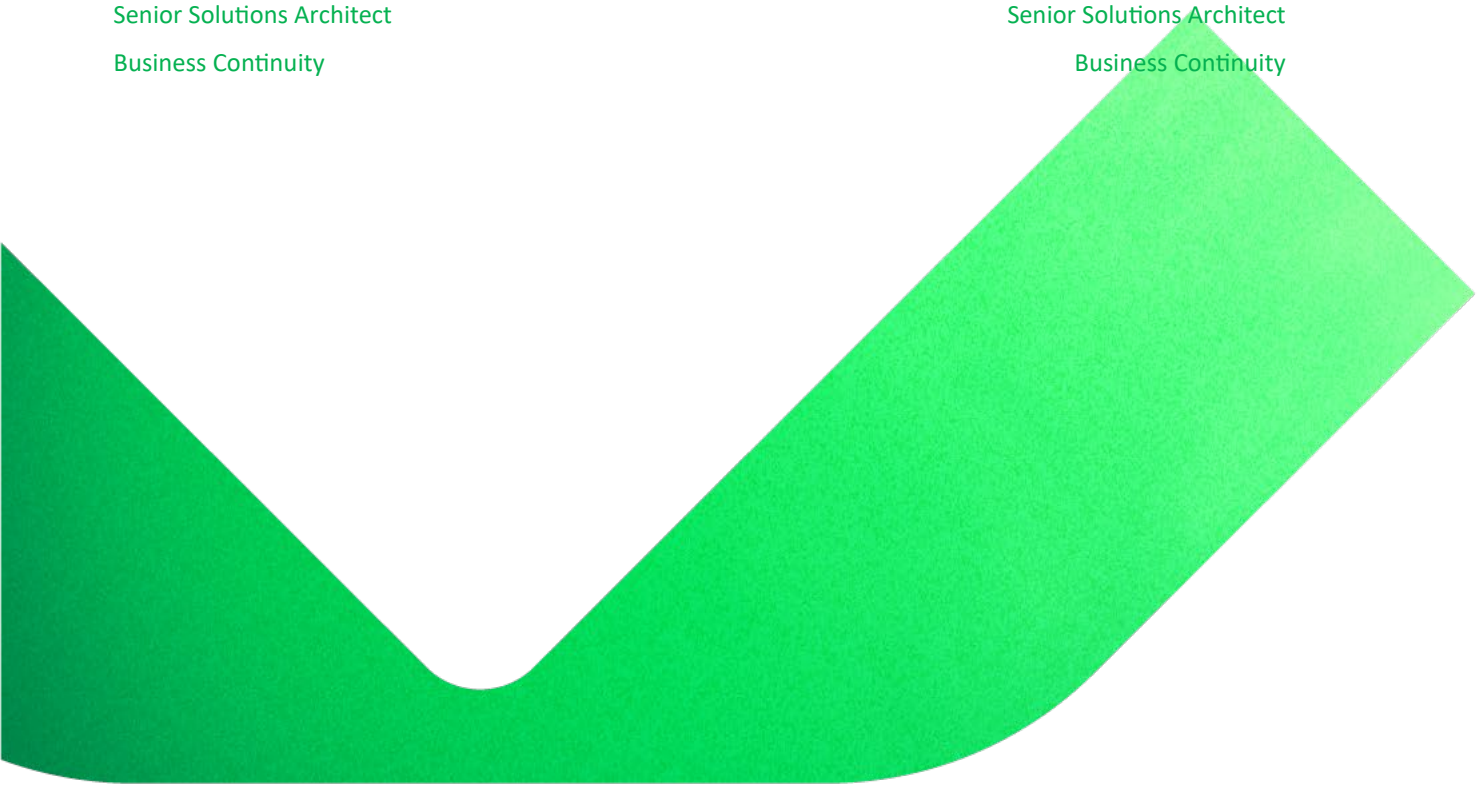
Business Continuity & Disaster Recovery Framework

2024

Matthias Mehrtens
Senior Solutions Architect
Business Continuity

Claudio Fortuna
Senior Solutions Architect
Business Continuity



Contents

V1.0 Matthias Mehrtens/Claudio Fortuna

Intended Audience

The intended audience includes business executives, IT managers, system administrators, data protection professionals, backup and recovery specialists, business continuity managers, and anyone involved in the planning and implementation of business continuity strategies.

I. Introduction to Business Continuity

In today's interconnected and dynamic business environment, organizations heavily rely on their operational infrastructure to function effectively and provide essential services.
However, with the growing complexity and potential vulnerabilities in various operational areas, such as physical infrastructure, supply chains, workforce, and processes, businesses face significant risks. These risks include natural disasters, supply chain disruptions, human errors, or external threats, which can lead to operational disruptions and result in substantial financial and reputational consequences.
To mitigate these risks and ensure uninterrupted business operations, organizations must establish a robust business continuity and disaster recovery strategy.

Who are the stakeholders?

Stakeholders in the context of business continuity refer to individuals or groups who have an interest or involvement in the organization's continuity of operations during a disruptive event.
The specific stakeholders can vary depending on the organization and its industry, but common stakeholders include:

Senior Management/Executives: Top-level executives who provide leadership, direction, and support for business continuity planning and decision-making.

Employees: All staff members within the organization who are responsible for implementing the business continuity strategies and procedures.

Customers/Clients: Individuals or organizations that rely on the products or services provided by the organization and may be impacted by disruptions.

Suppliers and Business Partners: External entities that provide goods, services, or support critical to the organization's operations and may need to be involved in the business continuity efforts.

Regulatory Authorities: Government bodies or agencies that oversee and regulate certain industries or sectors, setting standards and requirements for business continuity planning and compliance.

Shareholders/Investors: Individuals or organizations that have a financial stake in the organization's success and continuity of operations.

Legal and Compliance: Legal advisors or experts who ensure that the organization's business continuity plans align with applicable laws, regulations, and industry standards.

IT and Technology Teams: The IT department and technology specialists who are responsible for ensuring the availability and recovery of critical systems and data.

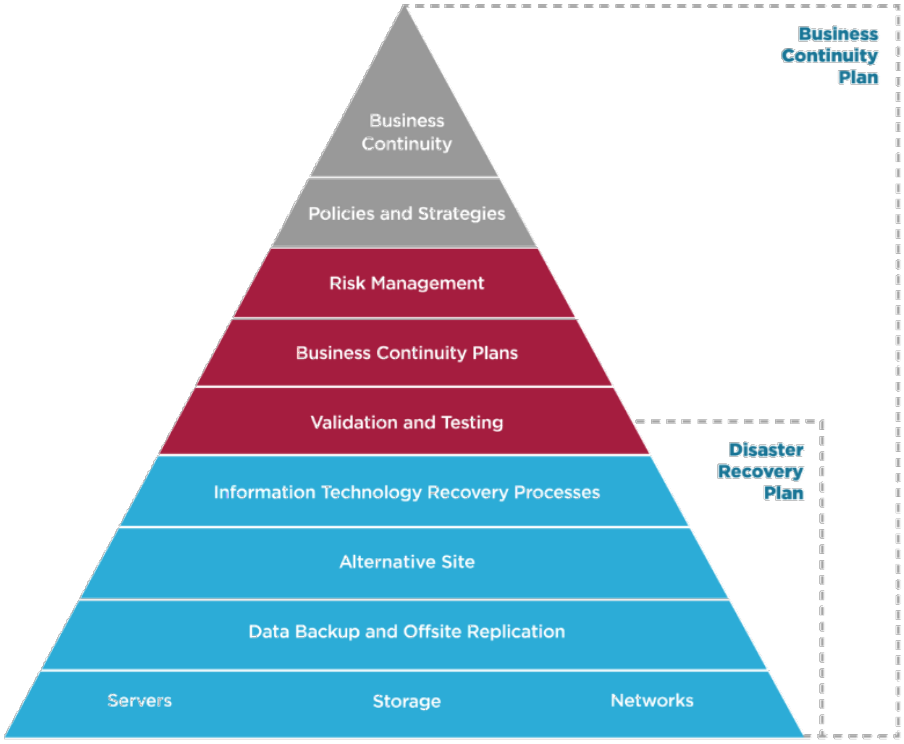
Facilities and Operations Teams: Teams responsible for maintaining the physical infrastructure, facilities, and operational processes of the organization.

Public Relations/Communications: Communication experts who handle external and internal communication during a crisis, ensuring transparency and maintaining the organization's reputation.

II. Overview of IT Business Continuity

IT Business Continuity refers to the strategies and plans put in place to ensure the availability, resilience, and recovery of critical IT systems, infrastructure, and data in the event of disruptions or disasters. It focuses on minimizing downtime, maintaining data integrity, and enabling uninterrupted business operations.

IT Disaster Recovery refers to the systematic process of restoring vital IT systems and infrastructure after a disruptive event. Its purpose is to minimize the impact of an IT-related incident, recover data and services, and restore normal operations swiftly and effectively.
IT DR is an essential component of an organization's risk management and business continuity strategy.



Key components such as **risk assessment**, **business impact analysis**, **recovery strategies**, **testing**, **documentation**, and **communication** work together to build resilience and effectively respond to disruptions, enabling organizations to navigate through crises with confidence.

By implementing comprehensive plans, organizations can safeguard their reputation and enjoy the numerous benefits associated with being prepared.

Main Goals of IT Business Continuity and Disaster Recovery

1. **Minimizing Downtime**: Any significant disruption to IT systems can result in costly downtime, leading to loss of productivity, revenue, and customer trust. IT business continuity plans help minimize downtime by providing predefined procedures for rapid recovery and restoration of essential services.
2. **Protecting Data**: Data is the lifeblood of modern organizations. IT disaster recovery ensures that data is backed up and can be recovered to prevent permanent loss, protecting sensitive information, intellectual property, and complying with regulatory requirements.
3. **Ensuring Business Continuity**: IT systems are critical for business operations. Effective business continuity plans enable organizations to maintain essential functions, deliver services, and meet customer expectations, even in the face of disruptions, meeting or exceeding predefined Service Level Agreements (SLAs) that dictate the expected levels of service availability, performance, and response time.
4. **Reducing Financial Losses**: Downtime, data loss, and damaged reputation can result in significant financial losses. IT business continuity helps minimize these losses by implementing preventive measures, ensuring prompt recovery, and reducing the financial impact of disruptions.

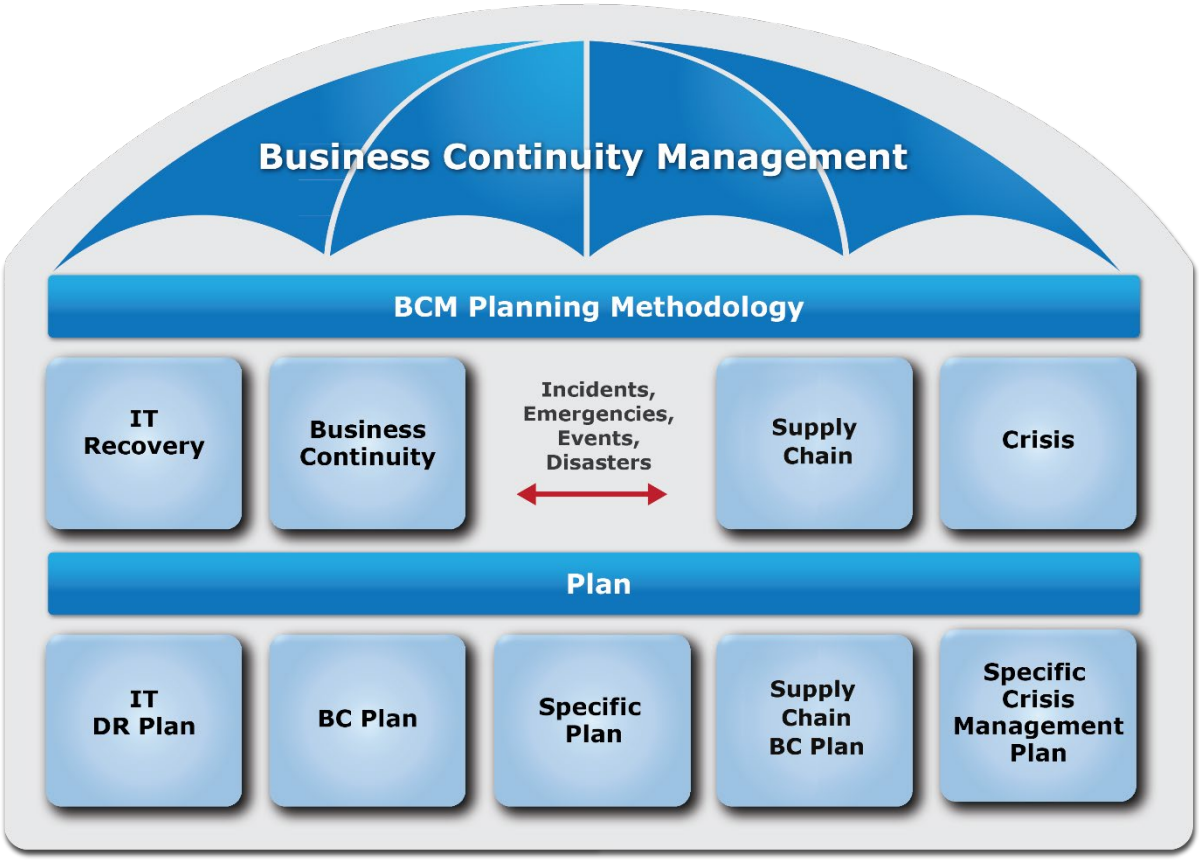
Implementing a robust IT business continuity strategy offers several significant benefits to organizations. First and foremost, it minimizes financial losses by reducing downtime and preventing revenue loss resulting from service interruptions, and helps organizations maintain regulatory compliance by ensuring the availability and integrity of critical data, the overall resilience of the organization is boosted reinforcing the ability to recover quickly and continue operations during challenging times.
Additionally, it provides peace of mind by reducing the uncertainty and potential chaos associated with IT disruptions; it instills confidence in stakeholders, including customers, partners, and employees, who depend on uninterrupted access to services and systems.

By investing in IT business continuity, organizations demonstrate their commitment to maintaining a stable and reliable IT infrastructure, which ultimately, strengthens their competitive advantage and reputation in the market.

Key components of IT Business Continuity and Disaster Recovery

1. **Risk Assessment**: Identify potential risks and threats that can impact IT systems, including natural disasters, cyber threats, human errors, and infrastructure failures. Assess their likelihood, potential impact, and prioritize them for mitigation.
2. **Business Impact Analysis (BIA)**: Analyze critical business processes, applications, and dependencies to determine their relative importance and potential impact on the organization in the event of a disruption. BIA helps prioritize recovery efforts and allocate resources effectively.
3. **Recovery Strategies**: Develop strategies and plans for recovering IT systems, applications, and data based on the risk assessment and BIA. This includes defining recovery time objectives (RTOs) and recovery point objectives (RPOs), considering options such as backup and restoration, failover to alternate systems, or cloud-based solutions.

4. **Backup and Data Protection**: Establish robust backup and data protection mechanisms, including regular backups, immutable copies, off-site storage, data encryption, and testing the integrity of backups to ensure data can be restored effectively.
5. **Redundancy and High Availability**: Deploy redundant infrastructure, such as clustered servers, load balancers, and data mirroring, to eliminate single points of failure and ensure continuous availability of critical IT services.
6. **Incident Response and Incident Management**: Establish protocols and procedures for quickly responding to IT incidents and managing their impact. This includes incident detection, communication, containment, investigation, and resolution.
7. **Testing and Exercising**: Regularly test the IT Business Continuity plans to validate their effectiveness and identify areas for improvement. This includes simulation exercises, tabletop drills, and full-scale recovery tests to assess the readiness of personnel, infrastructure, and processes.
8. **Monitoring and Maintenance**: Continuously monitor IT systems and infrastructure to detect potential vulnerabilities, performance issues, or security breaches. Regularly update and maintain IT Business Continuity plans to reflect changes in technology, business processes, and risks.
9. **Documentation and Communication**: Document all aspects of the IT Business Continuity plans, including procedures, roles, responsibilities, contact information, and escalation processes. Ensure clear communication channels and contact lists are readily available to facilitate prompt response and coordination during a crisis, and to keep key stakeholders informed during IT disruptions.
10. **Continuous Improvement**: The importance of ongoing improvement in IT Business Continuity efforts is essential. This involves learning from past incidents, implementing lessons learned, staying up to date with emerging technologies and industry best practices, and aligning IT Business Continuity strategies with evolving business needs.



III. ISO 22301 Standard

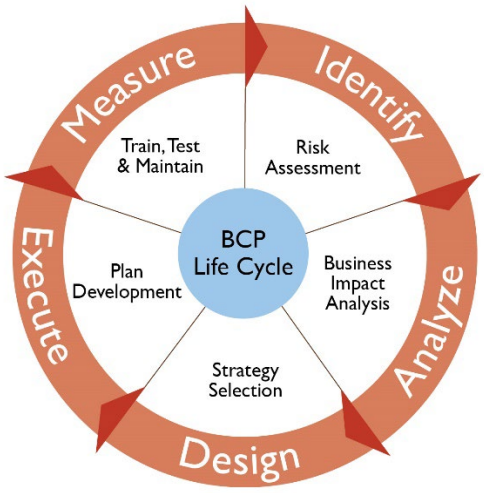
ISO 22301 is an internationally recognized standard that sets out the requirements for establishing, implementing, and maintaining a robust B***usiness Continuity Management System*** (BCMS). It is part of the ISO 22300 family of standards that focuses on security and resilience in various business domains.

ISO 22301 specifically addresses business continuity management, providing a systematic approach to identify potential threats, assess their impact, and implement measures to safeguard critical functions, services, and information.

Benefits of ISO 22301 certification

1. **Enhanced Resilience**: ISO 22301 helps organizations enhance their resilience by establishing a proactive framework to identify, assess, and mitigate risks. It promotes a culture of preparedness and enables timely response and recovery from disruptive events, minimizing the impact on business operations.
2. **Improved Business Continuity**: ISO 22301 ensures that organizations have effective plans and procedures in place to maintain critical functions and services during crises. By implementing business continuity management systems, organizations can minimize downtime, protect customer relationships, and maintain market reputation.
3. **Regulatory Compliance**: ISO 22301 helps organizations meet legal, regulatory, and contractual obligations related to business continuity and data protection. Compliance with this internationally recognized standard demonstrates a commitment to resilience and facilitates cooperation with partners and clients who prioritize secure and reliable business practices.
4. **Competitive Advantage**: Certification to ISO 22301 provides a competitive advantage by demonstrating to customers, partners, and stakeholders that the organization has robust business continuity management systems in place. It builds trust, instills confidence, and can differentiate the organization from competitors in the marketplace.

After establishing and implementing a BCMS based on the ISO 22301 framework, it is important to also maintain it continuously as the business evolves and changes. This results in a business continuity planning ***lifecycle***:



Identify: Organizations identify critical business functions, processes, and assets that are essential for their operations. This involves understanding dependencies, potential risks, and the impact of disruptions on these key components.

Analyze: Organizations conduct a detailed analysis of potential risks and threats that could disrupt their operations. This includes assessing the likelihood and potential impact of each risk, such as natural disasters, cyber-attacks, or supply chain disruptions.

Design: Based on the analysis, organizations design their business continuity strategies and plans. This includes determining recovery objectives, selecting appropriate recovery strategies, and designing processes to ensure continuity during a crisis.

Execute: In this phase, organizations create detailed business continuity plans that outline step-by-step procedures for responding to and recovering from disruptions. These plans include roles and responsibilities, communication protocols, and recovery procedures tailored to specific scenarios.

Measure: Following a disruption or recovery event, organizations measure the effectiveness of their business continuity efforts. This includes evaluating the response and recovery time, assessing the adherence to recovery objectives, and capturing lessons learned for future improvements.

Key requirements of ISO 22301

1. **Context of the Organization**: Organizations must determine the internal and external factors that may impact their business continuity management system. This includes understanding the organization's objectives, stakeholder requirements, and the business environment.
2. **Leadership and Commitment**: Top management must demonstrate leadership and commitment to the development, implementation, and continual improvement of the BCMS. They should define roles, responsibilities, and establish a business continuity policy that aligns with the organization's objectives.
3. **Planning**: Organizations must conduct a business impact analysis (BIA) and risk assessment to identify critical functions, dependencies, and potential threats. This information is used to develop business continuity objectives, strategies, and plans to ensure the timely recovery of operations.
4. **Support and Resources**: Adequate resources, competent personnel, and necessary infrastructure should be allocated to support the BCMS. Effective communication, awareness, and training programs should be implemented to ensure the organization's ability to respond to and recover from disruptions.
5. **Implementation and Operation**: This includes establishing processes and procedures for incident response, business continuity strategies, crisis management, and recovery operations. It involves implementing controls, conducting tests, and ensuring that documented procedures are in place.
6. **Performance Evaluation**: Organizations must monitor, measure, and evaluate the performance of the BCMS to ensure its effectiveness and continual improvement. This involves conducting regular audits, reviews, and exercising the BCMS to validate its performance and identify areas for enhancement.
7. **Continual Improvement**: Organizations should actively seek opportunities to improve the effectiveness of the BCMS by learning from incidents, monitoring emerging threats, and incorporating lessons learned into the planning and response processes.

Within the BCMS, IT disaster recovery (IT DR) holds a pivotal role.
IT DR focuses on ensuring the timely and effective recovery of IT systems, applications, and data in the event of a disruptive incident or disaster, encompassing strategies, processes, and procedures to minimize the impact of IT failures and restore critical business operations. The primary objective of IT DR is to enable the organization to recover its IT services and resume normal operations within acceptable timeframes and with minimal data loss.

ISO 22301 recognizes the interconnectedness between business processes and IT systems, emphasizing the need for an integrated approach to BCM. IT DR is a key component of this integration, providing the necessary technical capabilities and mechanisms to support the overall business continuity objectives, ensuring the availability and recovery of critical IT systems, applications, and data, and supporting the overall objective of maintaining business continuity in the face of disruptive incidents.

Strategy and Planning / Leadership commitment

Leadership commitment refers to the active involvement and support of top management in establishing and maintaining a business continuity management system (BCMS) within an organization.

Leadership is responsible for:

1. Ensuring BCM objectives aligned with corporate objectives
2. Ensuring BCM requirements integrated into business functions
3. Ensuring availability of BCM resources
4. Providing support to BCM activities
5. Ensuring BCM achieves its objectives
6. Promoting continuous improvement

Leadership commitment is imperative to the BCM program success.

In order to initiate a successful BCM program, organizations should follow these strategic steps:

- **Establish the Need for the BCM Program**: This involves identifying the drivers that necessitate a business continuity management (BCM) program, such as regulatory requirements, industry best practices, audit reports highlighting vulnerabilities, or benchmark standards. Understanding these factors helps justify the importance and relevance of implementing a BCM program.
- **Establish Purpose and Objectives**: Clearly define the purpose and objectives of the BCM program, both from a strategic and operational perspective. This includes identifying the desired outcomes, such as ensuring continuity of critical business functions, minimizing disruptions, protecting assets, and maintaining customer trust.
- **Build the Business Continuity Framework**: Develop the framework for the BCM program, including its scope, key components, and roles and responsibilities of personnel involved. Define the organizational structure, communication channels, and reporting mechanisms to ensure effective coordination and implementation of the program.
- **Establish Program Implementation Plan, Resources, and Timelines**: Create a detailed plan that outlines the steps, activities, and timelines for implementing the BCM program. Determine the necessary resources, including personnel, budget, and technology, to support the program's successful execution.
- **Obtain Management Approval and Funding Support**: Seek formal approval from top management to initiate the BCM program. Present a compelling case highlighting the benefits, cost-effectiveness, and alignment with organizational goals. Secure the necessary funding and resources to support the program's implementation and ongoing maintenance.

Risk Assessment

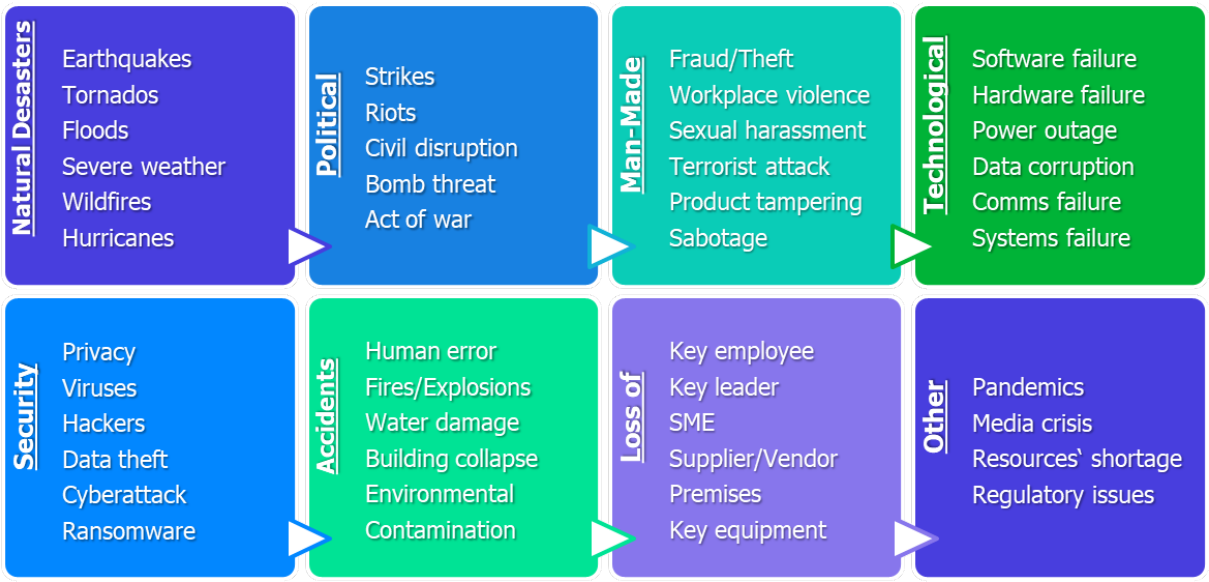
The risk assessment process is a crucial component of business continuity management. It involves the identification, analysis and evaluation of potential risks and their potential impact on an organization's ability to achieve its objectives.
The risk assessment aims to provide an understanding of the risks faced by the organization, allowing informed decision-making and the development of appropriate risk mitigation strategies.

The risk assessment starts with a structured approach, which includes the following questions:

1. What could happen? **(Risk)**
2. How could it happen? **(Cause)**
3. What is the likelihood? **(Probability)**
4. What could be the consequences? **(Impact)**
5. Is there anything that could be done to reduce likelihood or consequences? **(Controls)**

The **risk** is connected to the **cause**: a major incident in security, an accident of some sort, any natural disaster will pose a risk to the continuity of the activities.

The common types of disasters that could happen includes:



Disasters can often have interconnected or cascading effects, meaning that one event can trigger or exacerbate another.
For each kind of disaster the organization should:

a) identify the risks of disruption to the organization's prioritized activities and to their required resources

b) analyze and evaluate the identified risks

c) determine which risks require treatment

The evaluation criteria are based on:

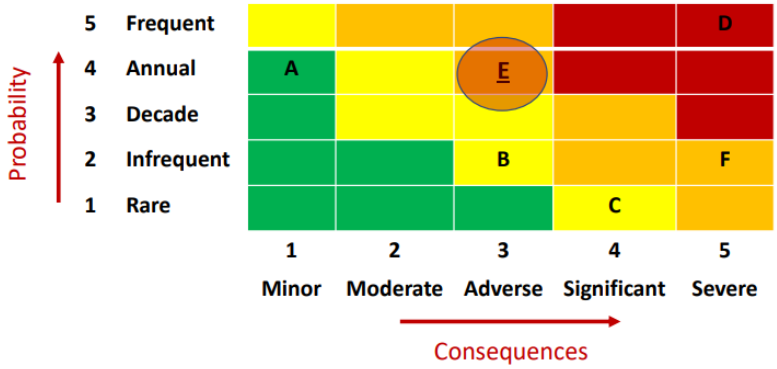
Probability - the likelihood of an event, or the likelihood of a specified consequence.

Frequency	Description	Score
Frequent	more than once per year	5
Annual	once per year	4
Decade	at least once every 10 years	3
Infrequent	once in 10-20 years	2
Rare	once in >20 years	1

Impact - Qualitative or quantitative assessment of the outcome.

	Financial	Non-Financial		
		Customer/Operational	Reputational	Legal/Regulatory
Minor (1)	< $ 100k	Risk confined to 1 customer	Minor impact (client complains)	Requires regulatory notification only
Moderate (2)	$ 101k – $ 500k			Minor fine
Adverse (3)	$ 501k – $ 1M	Risk affects a specific group	Mass social media spread	Risk can result in substantial regulatory fine
Significant (4)	$ 1.1M – $ 3M			Regulatory breach, substantial fine is inevitable
Severe (5)	➢ $ 3M	Risk impacts all customers	Global wide-spread scandal	Risk can result in license suspension

The resulting analysis produces a table with a score that maps to a Low, Medium, High or Critical Risk, allowing informed decision-making and the development of appropriate risk mitigation strategies (**control**).



Inherent Risk

Risk	Prob.	Impact	Score
A	4	1	4
B	2	3	6
C	1	4	4
D	5	5	25
E	4	3	12
F	2	5	10

A control is any action taken by management to reduce risk and enhance the likelihood that objectives will be achieved.

• Control Activities – Policies and procedures establish actions to effectively manage risks and safeguard the achievement of objectives.

Control type	Description	Examples
Preventive	deter undesirable events from occuring	System access, system checks, passwords
Detective / Corrective	to detect and correct undesirable events that have happened	Reconciliation
Directive	to cause or encourage a desirable event to occur	Policies, procedures, manuals, etc.

• Control Assessment – Evaluate whether a set of controls is sufficient to mitigate the identified risks.

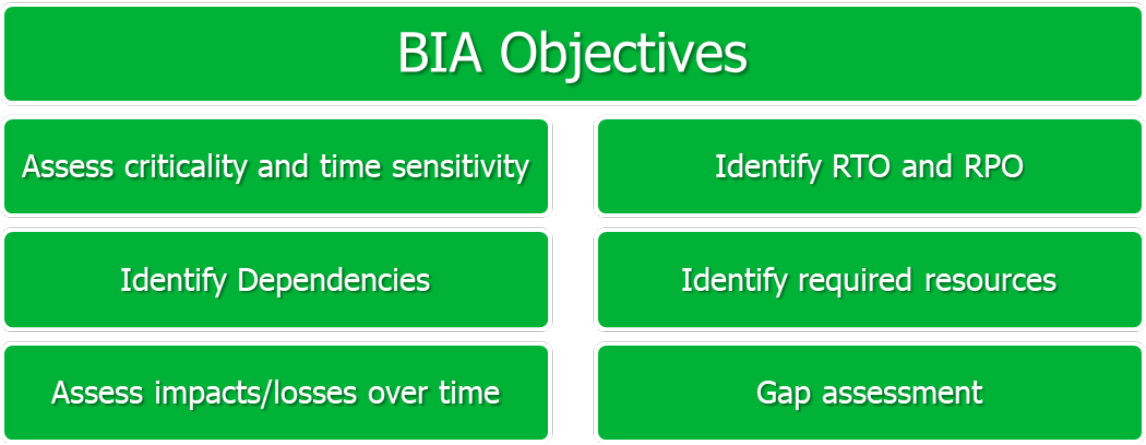
Controls	Criteria
Effective	Controls are effective 100% of the time
Mostly Effective	Controls are effective 80-99% of the time
Partially Effective	Controls are effective 50-79% of the time
Not Effective	Controls are effective <50% of the time

This assessment relies heavily on professional expertise, as there is limited information available to guide the evaluation process.

Business Impact Analysis

Business Impact Analysis (BIA) is a systematic process that assesses the potential consequences of disruptions to critical business functions. It aims to identify and prioritize key activities, understand their dependencies, and evaluate the impact of their disruption on the organization.

The BIA helps organizations determine appropriate business continuity strategies and allocate resources effectively to minimize the impact of disruptions on their operations.



The Business Impact Analysis includes the following steps:

1. **Assess criticality and time sensitivity** - Assessment of function/activities prioritized and identified between:
    - *Mission critical*: must be available for the organization to operate (eg. Key IT systems, Finance, etc)
    - *Essential*: important in the short term but won't immediately halt operations (eg. emails)
    - *Important*: important but not in the short term (eg. Payroll)
    - *Minor*: can be recovered over longer time frame without significant impact (ex. Other IT, HR)
2. **Identify dependencies** - Chart interdependencies between different processes, systems, resources, and stakeholders that contribute to the successful execution of critical business functions or activities. By identifying these dependencies, organizations can assess the potential ripple effects of disruptions and determine the extent of impact on other functions.
3. **Identify impacts/losses over time** - Identify the qualitative and quantitative criteria to assess the impact:
    - *Customer Impact*: Service level, loss of customers, complaints
    - *Financial Impact*: Loss of profits, market share, Contractual fines or penalties
    - *Regulatory impact:* Fines, Revocation of license, Termination of business
    - *Operational impact:* Workflow and Supply chain disruptions
    - *Reputational impact:* Media attention, Loss of shareholder confidence
    - *Human impact:* Loss of life and injury, compensation claims
4. **Identify RTO and RPO** – Recovery Time Objectives (RTO) is the maximum amount of time that the business function can be suspended before causing disruption of operations "acceptable downtime".
   When assessing applications, it is important to identify their Recovery Point Objectives (RPOs), which indicate the maximum acceptable data loss for an activity to resume operations after a disruption.
   The RTO & RPO should be established at the entity function or process level.

5. **Identify Required Resources** - Assess the resources required to support recovery objectives, like:
    - *Critical staff requirements*
    - *Critical equipment*: PCs, laptop, phones, printers, machinery, etc
    - *Critical facilities*: alternate sites
    - *Critical systems/applications, backup servers*
    - *Critical Third parties, vendors or suppliers:* standby agreements
6. **Gap Assessment** - Identify any discrepancies or shortcomings in the organization's current state of preparedness for potential disruptions:
    - Identify and gaps between available (existing resources) and the BIA resource requirements.
    - Discuss with business leaders and stakeholders
    - Obtain budget approval

Defining Business continuity strategies

Defining business continuity strategies involves developing approaches and plans to mitigate the impact of disruptions and ensure the continuity of critical business functions. This includes identifying and implementing preventive, detective, and corrective controls to minimize the likelihood and consequences of disruptions.
The strategies encompass various aspects such as backup and recovery procedures, alternate site arrangements, communication protocols, resource allocation, and incident response mechanisms.

The goal is to establish a comprehensive framework that outlines the actions to be taken during a disruption, enabling organizations to effectively manage and recover from incidents while minimizing the impact on business operations.

These are the steps for building a Business Continuity strategy:

1. **Review the recovery requirements** identified for each of the entity's operational areas
2. **Identify alternative business continuity strategies**, like manual workaround procedures, alternate sites, third party service providers
3. **Assess viability of alternative strategies** against the results of business impact analysis
4. **Address supply chain issues** affecting recovery strategies
5. **Identify possible Business Interruption** – evaluate BI Insurance coverage*
6. **Identify technology failover capabilities**, like dual data centers
7. **Identify strategies for data recovery** that meets RPO requirements
8. **Review and assess supply chain recovery capabilities**
9. **Strategy Cost Benefit Analysis**, what's the cost required for implementation
10. **Recommend Strategies** and **Obtain Approval**, presenting the information to the leadership team

*BI Insurance coverage is a type of insurance that provides financial protection to businesses in the event of an interruption to their normal operations. It is designed to cover the loss of income and additional expenses incurred by a business due to a covered peril, such as fire, natural disaster, or other unforeseen events.

Creating the BCP Framework

The organization should implement and maintain a response structure that will enable timely warning and communication to relevant interested parties.
It should provide plans and procedures to manage the organization during a disruption.
The plans and procedures are to be used when required, to activate business continuity solutions.

Following the preparation of approved strategies in the previous step, the successive task requires to:

1. **Document plans** to be used during incident that will enable the entity to continue to function.
2. **Institutionalize** the teams, actions and outsourced services
3. **Familiarize all employees** into the new backup and recovery strategies and technologies.

A comprehensive Business Continuity Plan should cover:

Purpose and Scope: Clearly defines the objectives and scope of the BCP, specifying which business functions and activities are covered.

Objectives: States the desired outcomes of the BCP, such as minimizing downtime, ensuring employee safety, safeguarding critical data, and maintaining customer service levels.

Activation Criteria and Procedures: Defines the triggers or conditions that indicate when the BCP should be activated and outlines the steps and protocols to follow when activating the plan.

Implementation Procedures & Timelines: Provides detailed instructions on how to execute the BCP, including the sequence of actions, timelines for implementation, and coordination with relevant stakeholders.

Roles and Responsibilities: Assigns specific roles and responsibilities to individuals or teams involved in the BCP, clarifying who is accountable for various tasks and decision-making during a disruption.

Communication Procedures: Outlines the communication channels, protocols, and contact information for internal and external stakeholders, ensuring effective and timely communication during an incident.

Interdependencies: Identifies the dependencies between different business functions, systems, suppliers, and stakeholders to highlight critical interrelationships that need to be considered during recovery efforts.

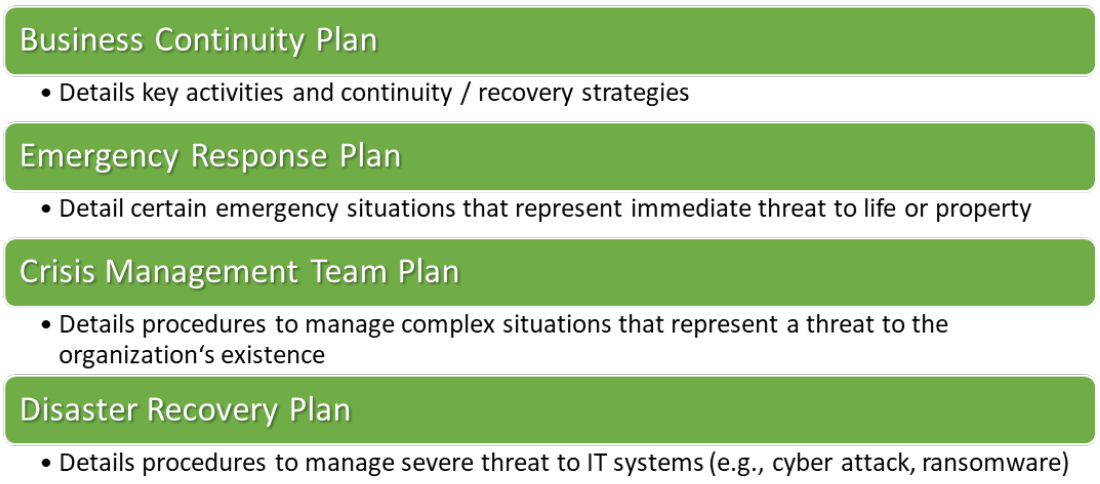
Resource Requirements: Specifies the resources, such as personnel, equipment, facilities, and technology, needed to execute the BCP effectively.

Documentation and Governance Process: Describes how the BCP is documented, maintained, reviewed, and updated over time, including the governance structure and responsibilities for ensuring the plan's accuracy and relevance.

The documentation of the business continuity plan should prioritize clarity and eliminate any potential confusion or ambiguity.
The plan should answer the following questions clearly:

1. **Who?** The person/s who performs the recovery
2. **What?** The actions to be taken
3. **When?** The order of procedures
4. **Where?** The place where the recovery will occur
5. **How?** Resources, suppliers, and business partners that will be involved

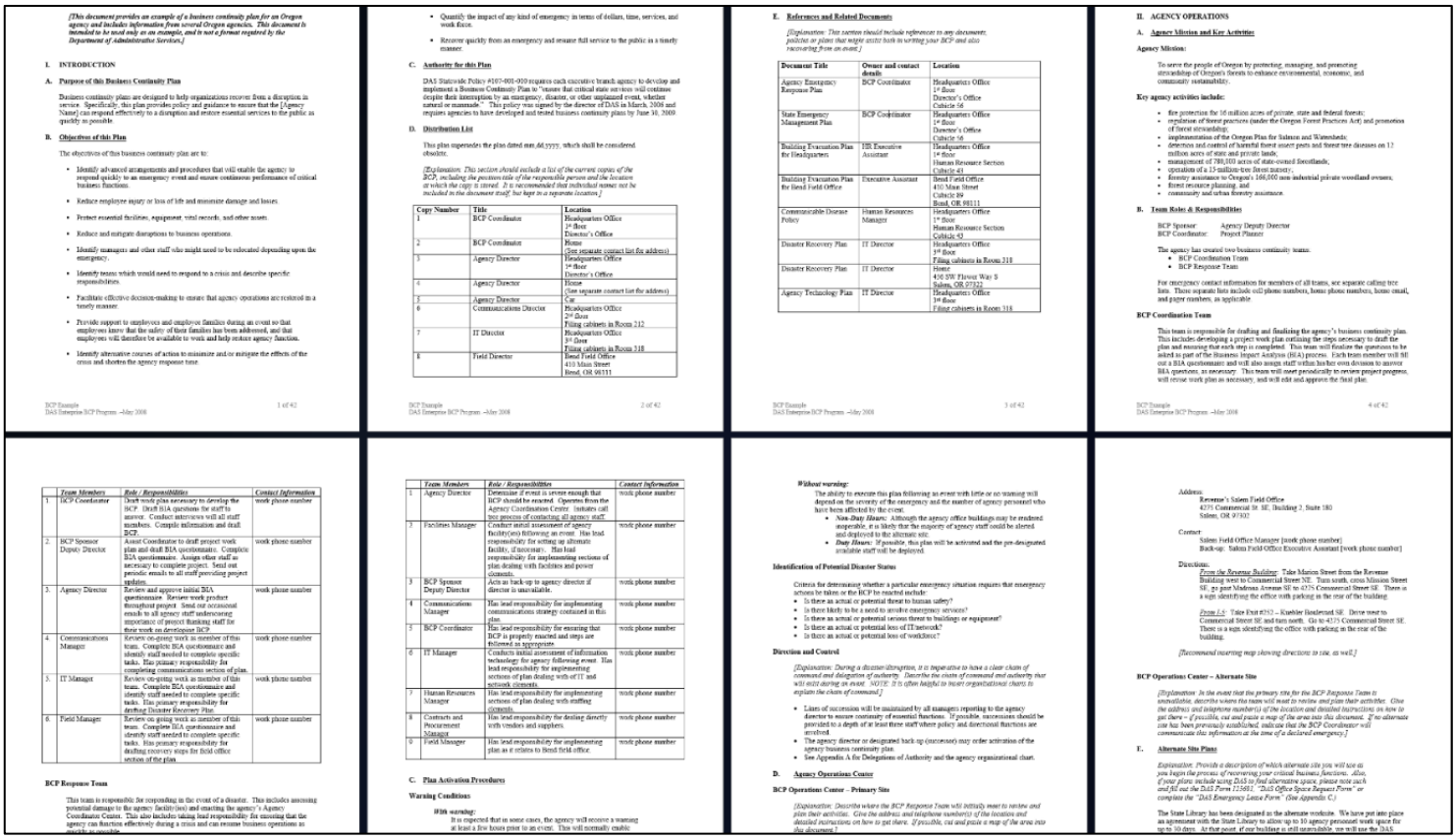
There are several types of business continuity plans. The key types are as follows:



The final step is to publish the Plan Documents:

1. Provide final draft to business process owners
2. Obtain authorized signatures
3. Publish and distribute plan to stakeholders, business owners and BCP support team
4. Establish procedures for distribution and control of plans (e.g., distribution list) including plan changes and updates guidelines.

Following is a sample Business Continuity Recovery Plan by State of Oregon (full document can be found here):



[This document provides an example of a business continuity plan for an Oregon agency and includes information from several Oregon agencies. This document is intended to be used only as an example, and is not a format required by the Department of Administrative Services.]

I. INTRODUCTION

A. Purpose of this Business Continuity Plan

Business continuity plans are designed to help organizations recover from a disruption in service. Specifically, this plan provides policy and guidance to ensure that the [Agency Name] can respond effectively to a disruption and restore essential services to the public as quickly as possible.

B. Objectives of this Plan

The objectives of this business continuity plan are to:

- Identify advanced arrangements and procedures that will enable the agency to respond quickly to an emergency event and ensure continuous performance of critical business functions.
- Reduce employee injury or loss of life and minimize damage and losses.
- Protect essential facilities, equipment, vital records, and other assets.
- Reduce and mitigate disruptions to business operations.
- Identify managers and other staff who might need to be relocated depending upon the emergency.
- Identify teams which would need to respond to a crisis and describe specific responsibilities.
- Facilitate effective decision-making to ensure that agency operations are restored in a timely manner.
- Provide support to employees and employee families during an event so that employees know that the safety of their families has been addressed, and that employees will therefore be available to work and help restore agency function.
- Identify alternative courses of action to minimize and/or mitigate the effects of the crisis and shorten the agency response time.

BCP Example
DAS Enterprise BCP Program –May 2008
1 of 42

- Quantify the impact of any kind of emergency in terms of dollars, time, services, and work force.
- Recover quickly from an emergency and resume full service to the public in a timely manner.

C. Authority for this Plan

DAS Statewide Policy #107-001-010 requires each executive branch agency to develop and implement a Business Continuity Plan to "ensure that critical state services will continue despite their interruption by an emergency, disaster, or other unplanned event, whether natural or manmade." This policy was signed by the director of DAS in March, 2008 and requires agencies to have developed and tested business continuity plans by June 30, 2009.

D. Distribution List

This plan *supersedes* the plan dated mm.dd.yyyy, which shall be considered obsolete.

[Explanation: This section should include a list of the current copies of the BCP, including the position title of the responsible person and the location at which the copy is stored. It is recommended that individual names not be included in the document itself, but kept in a separate location.]

Copy Number	Title	Location
1	BCP Coordinator	Headquarters Office 1st floor Director's Office
2	BCP Coordinator	Home (See separate contact list for address)
3	Agency Director	Headquarters Office 1st floor Director's Office
4	Agency Director	Home (See separate contact list for address)
5	Agency Director	Car
6	Communications Director	Headquarters Office 2nd floor Filing cabinets in Room 212
7	IT Director	Headquarters Office 3rd floor Filing cabinets in Room 318
8	Field Director	Bend Field Office 410 Main Street Bend, OR 98331

BCP Example
DAS Enterprise BCP Program –May 2008
2 of 42

E. References and Related Documents

[Explanation: This section should include references to any documents, policies or plans that might assist both in writing your BCP and also recovering from an event.]

Document Title	Owner and contact details	Location
Agency Emergency Response Plan	BCP Coordinator	Headquarters Office 1st floor Director's Office Cubicle 56
State Emergency Management Plan	BCP Coordinator	Headquarters Office 1st floor Director's Office Cubicle 56
Building Evacuation Plan for Headquarters	HR Executive Assistant	Headquarters Office 1st floor Human Resource Section Cubicle 43
Building Evacuation Plan for Bend Field Office	Executive Assistant	Bend Field Office 410 Main Street Cubicle 89 Bend, OR 98331
Communicable Disease Policy	Human Resources Manager	Headquarters Office 1st floor Human Resource Section Cubicle 93
Disaster Recovery Plan	IT Director	Headquarters Office 3rd floor Filing cabinets in Room 318
Disaster Recovery Plan	IT Director	Home 436 SW Flower Way S Salem, OR 97322
Agency Technology Plan	IT Director	Headquarters Office 3rd floor Filing cabinets in Room 318

BCP Example
DAS Enterprise BCP Program –May 2008
3 of 42

II. AGENCY OPERATIONS

A. Agency Mission and Key Activities

Agency Mission:

To serve the people of Oregon by protecting, managing, and promoting stewardship of Oregon's forests to enhance environmental, economic, and community sustainability.

Key agency activities include:

- fire protection for 16 million acres of private, state and federal forests;
- regulation of forest practices (under the Oregon Forest Practices Act) and promotion of forest stewardship;
- implementation of the Oregon Plan for Salmon and Watersheds;
- detection and control of harmful forest insect pests and forest tree diseases on 12 million acres of state and private lands;
- management of 780,000 acres of state-owned forestlands;
- operation of a 13-million-tree forest nursery;
- forestry assistance to Oregon's 166,000 non-industrial private woodland owners;
- forest resource planning; and
- community and urban forestry assistance.

B. Team Roles & Responsibilities

BCP Sponsor: Agency Deputy Director
BCP Coordinator: Project Planner

The agency has created two business continuity teams:

- BCP Coordination Team
- BCP Response Team

For emergency contact information for members of all teams, see separate callout text lists. Three separate lists include cell phone numbers, home phone numbers, home email, and pager numbers, as applicable.

BCP Coordination Team

This team is responsible for drafting and finalizing the agency's business continuity plan. This includes developing a project work plan outlining the steps necessary to draft the plan and ensuring that each step is completed. This team will finalize the questions to be asked as part of the Business Impact Analysis (BIA) process. Each team member will fill out a BIA questionnaire and will also assign staff within his/her own division to answer BIA questions, as necessary. This team will meet periodically to review project progress, will revise work plan as necessary, and will edit and approve the final plan.

BCP Example
DAS Enterprise BCP Program –May 2008
4 of 42

	Team Members	*Role / Responsibilities*	*Contact Information*
1.	BCP Coordinator	Draft work plan necessary to develop the BCP. Draft BIA questions for staff to answer. Conduct interviews with all staff members. Compile information and draft BCP.	work phone number
2.	BCP Sponsor Deputy Director	Assist Coordinator to draft project work plan and draft BIA questionnaire. Complete BIA questionnaire. Assign other staff as necessary to complete project. Send out periodic emails to all staff providing project updates.	work phone number
3.	Agency Director	Review and approve initial BIA questionnaire. Review work product throughout project. Send out occasional emails to all agency staff underscoring importance of project thanking staff for their work on development BCP.	work phone number
4.	Communications Manager	Reviews on-going work as member of this team. Complete BIA questionnaire and identify staff needed to complete specific tasks. Has primary responsibility for completing communications section of plan.	work phone number
5.	IT Manager	Reviews on-going work as member of this team. Complete BIA questionnaire and identify staff needed to complete specific tasks. Has primary responsibility for drafting Disaster Recovery Plan.	work phone number
6.	Field Manager	Reviews on-going work as member of this team. Complete BIA questionnaire and identify staff needed to complete specific tasks. Has primary responsibility for drafting recovery steps for field office section of the plan.	work phone number

BCP Response Team

This team is responsible for responding in the event of a disaster. This includes assessing potential damage to the agency facility(ies) and enacting the agency's Agency Coordinator Center. This also includes taking lead responsibility for ensuring that the agency can function effectively during a crisis and can resume business operations as quickly as possible.

	Team Members	*Role / Responsibilities*	*Contact Information*
1	Agency Director	Determine if event is severe enough that BCP should be enacted. Operates from the Agency Coordination Center. Initiates call tree process of contacting all agency staff.	work phone number
2	Facilities Manager	Conduct initial assessment of agency facility(ies) following an event. Has lead responsibility for setting up alternate facility, if necessary. Has lead responsibility for implementing sections of plan dealing with facilities and power elements.	work phone number
3	BCP Sponsor Deputy Director	Acts as back-up to agency director if director is unavailable.	work phone number
4	Communications Manager	Has lead responsibility for implementing communications strategy contained in this plan.	work phone number
5	BCP Coordinator	Has lead responsibility for ensuring that BCP is properly enacted and steps are followed as appropriate.	work phone number
6	IT Manager	Conducts initial assessment of information technology for agency following event. Has lead responsibility for implementing sections of plan dealing with IT and network elements.	work phone number
7	Human Resources Manager	Has lead responsibility for implementing sections of plan dealing with staffing elements.	work phone number
8	Contracts and Procurement Manager	Has lead responsibility for dealing directly with vendors and suppliers.	work phone number
9	Field Manager	Has lead responsibility for implementing plan as it relates to Bend field office.	work phone number

C. Plan Activation Procedures

Warning Conditions

With warning:
It is expected that in some cases, the agency will receive a warning at least a few hours prior to an event. This will normally enable

Without warning:
The ability to execute this plan following an event with little or no warning will depend on the severity of the emergency and the number of agency personnel who have been affected by the event.

- ***Non-Duty Hours:*** Although the agency office buildings may be rendered inoperable, it is likely that the majority of agency staff could be alerted and deployed to the alternate site.
- ***Duty Hours:*** If possible, this plan will be activated and the pre-designated available staff will be deployed.

Identification of Potential Disaster Status

Criteria for determining whether a particular emergency situation requires that emergency actions be taken or the BCP be enacted include:

- Is there an actual or potential threat to human safety?
- Is there likely to be a need to involve emergency services?
- Is there an actual or potential serious threat to buildings or equipment?
- Is there an actual or potential loss of IT network?
- Is there an actual or potential loss of workforce?

Direction and Control

[Explanation: During a disaster/disruption, it is imperative to have a clear chain of command and delegation of authority. Describe the chain of command and authority that will exist during an event. NOTE: It is often helpful to insert organizational charts to explain the chain of command.]

- Lines of succession will be maintained by all managers reporting to the agency director to ensure continuity of essential functions. If possible, successors should be provided to a depth of at least three staff where policy and directional functions are involved.
- The agency director or designated back-up (successor) may order activation of the agency business continuity plan.
- See Appendix A for Delegation of Authority and the agency organizational chart.

D. Agency Operations Center

BCP Operations Center – Primary Site

[Explanation: Describe where the BCP Response Team will initially meet to review and plan their activities. Give the address and telephone number(s) of the location and detailed instructions on how to get there. If possible, cut and paste a map of the area into this document.]

Address:
Revenue's Salem Field Office
4275 Commercial St. SE, Building 2, Suite 180
Salem, OR 97302

Contact:
Salem Field Office Manager [work phone number]
Back-up: Salem Field Office Executive Assistant [work phone number]

Directions:
From the Revenue Building: Take Marion Street from the Revenue Building west to Commercial Street NE. Turn south, cross Mission Street SE, to past Madrona Avenue SE to 4275 Commercial Street SE. There is a sign identifying the office with parking in the rear of the building.

From I-5: Take Exit #253 – Kuebler Boulevard SE. Drive west to Commercial Street SE and turn north. Go to 4275 Commercial Street SE. There is a sign identifying the office with parking in the rear of the building.

[Recommend inserting map showing directions to site, as well.]

BCP Operations Center – Alternate Site

[Explanation: In the event that the primary site for the BCP Response Team is unavailable, describe where the team will meet to review and plan their activities. Give the address and telephone number(s) of the location and detailed instructions on how to get there – if possible, cut and paste a map of the area into this document. If no alternate site has been previously established, indicate that the BCP Coordinator will communicate this information at the time of a declared emergency.]

E. Alternate Site Plans

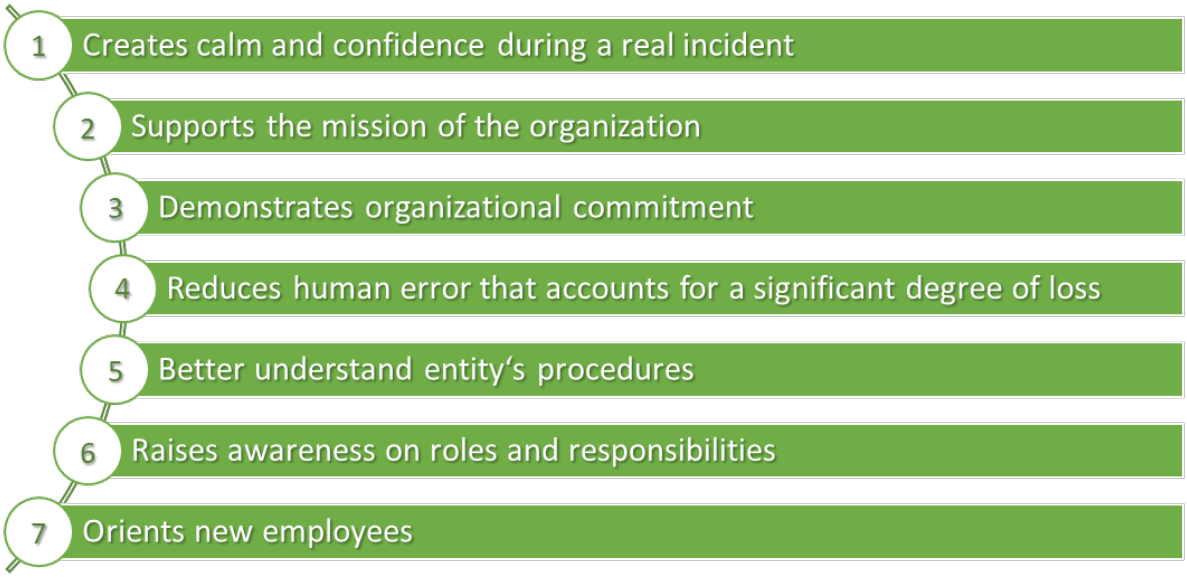
Explanation: Provide a description of which alternate site you will use as you begin the process of recovering your critical business functions. Also, if your plans include using DAS to find alternative space, please note such and fill out the DAS Form 125682, "DAS Office Space Request Form" or complete the "DAS Emergency Lease Form" (See Appendix C.)

The State Library has been designated as the alternate worksite. We have put into place an agreement with the State Library to allow up to 10 agency personnel work space for up to 30 days. At that point, if our building is still unavailable, we will use the DAS

Please notice the sections outlining the **Purpose**, **Objectives**, **Distribution List**, the documents related to the **BCP**, the **BCP Coordination** and response team, and the **Plan Activation Procedures**.

Awareness and Training Programs

By fostering a culture of preparedness, awareness and training programs ensure that employees understand their roles and responsibilities during disruptive events. Such programs contribute to increased employee engagement, accountability, and overall organizational resilience. Additionally, awareness campaigns and training sessions help to minimize the negative impact of incidents by enabling employees to respond promptly and effectively.



The primary objectives of awareness and training programs within the IS22301 standard include:

1. **Promoting Understanding**: Increase awareness of business continuity principles, terminology, and concepts among employees across all levels of the organization.
2. **Building Competency**: Equip employees with the necessary skills and knowledge to perform their roles effectively during a crisis, including incident response, communication protocols, and recovery procedures.
3. **Enhancing Collaboration**: Foster cross-functional collaboration and coordination, ensuring that individuals understand their interconnectedness and can work seamlessly to maintain critical operations.
4. **Instilling Confidence**: Boost employee confidence by providing them with the necessary tools and training to handle disruptive events, minimizing panic and facilitating a structured response.

To effectively implement awareness and training programs, organizations should consider the following key elements:

1. **Needs Assessment**: Conduct a thorough analysis of the organization's awareness and training requirements, considering job roles, functions, and critical processes. Identify knowledge gaps and prioritize areas for improvement.
2. **Program Development**: Design a comprehensive program that aligns with the organization's objectives and the IS22301 standard. This includes creating content, selecting appropriate training methods (e.g., workshops, e-learning), and determining the frequency and duration of training sessions.
3. **Training Delivery**: Implement the program by delivering training to employees across different levels of the organization. Use a variety of engaging methods to cater to different learning styles and ensure active participation. This can include scenario-based exercises, simulations, and tabletop drills.

4. **Documentation and Records**: Maintain thorough documentation of training materials, attendance records, and assessment results. This documentation serves as evidence of compliance and helps identify areas for improvement in future training initiatives.
5. **Communication and Awareness**: Develop a communication strategy to raise awareness about the importance of business continuity and the role each employee plays in ensuring organizational resilience. Regularly communicate updates, best practices, and success stories to reinforce a culture of preparedness.
6. **Training Evaluation**: Continuously assess the effectiveness of the training program by soliciting feedback from participants, monitoring performance during exercises, and conducting post-training evaluations. Use this information to make necessary adjustments and improvements.

Exercise, Assessment, and Maintenance

The exercise, assessment and maintenance activities provide organizations with the opportunity to validate the effectiveness of their plans, identify gaps in their strategies, and build confidence in their ability to respond to disruptions. By conducting regular exercises and assessments, organizations can evaluate their preparedness and identify areas for improvement. Moreover, maintenance ensures that business continuity plans remain up-to-date, relevant, and aligned with changes in the organization's structure, processes, and external environment. These activities not only demonstrate a commitment to resilience but also contribute to minimizing the impact of incidents on the organization's operations, reputation, and customer trust.

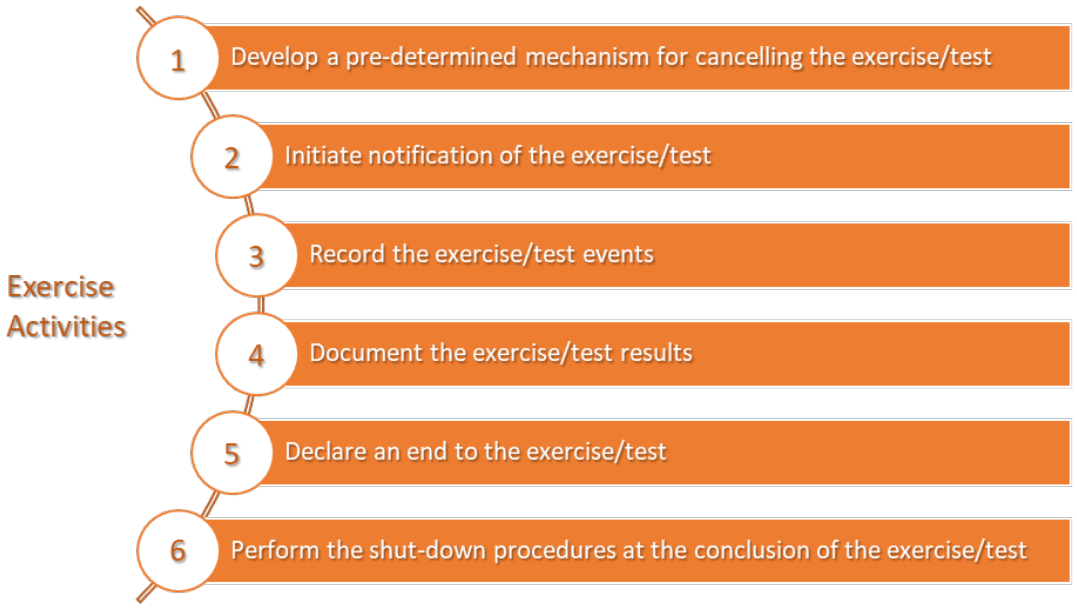
The primary objectives of exercise, assessment, and maintenance practices in the IS22301 standard are as follows:

1. **Validate Preparedness**: Conduct exercises to test the effectiveness of the Business Continuity Management system, ensuring that plans and procedures can be implemented successfully in real-life scenarios.
2. **Identify Weaknesses**: Through assessments, identify gaps, vulnerabilities, and weaknesses in the organization's response capabilities, enabling targeted improvements and corrective actions.
3. **Promote Learning and Training**: Exercises and assessments provide valuable learning opportunities for employees and key stakeholders, helping them gain practical experience and reinforcing training efforts.
4. **Enhance Coordination**: By simulating crisis situations, exercises foster cross-functional coordination and collaboration, improving communication and synergy during actual incidents.
5. **Maintain Currency**: Regular maintenance activities ensure that business continuity plans remain current, reflecting changes in the organization's operations and external factors that may impact continuity efforts.

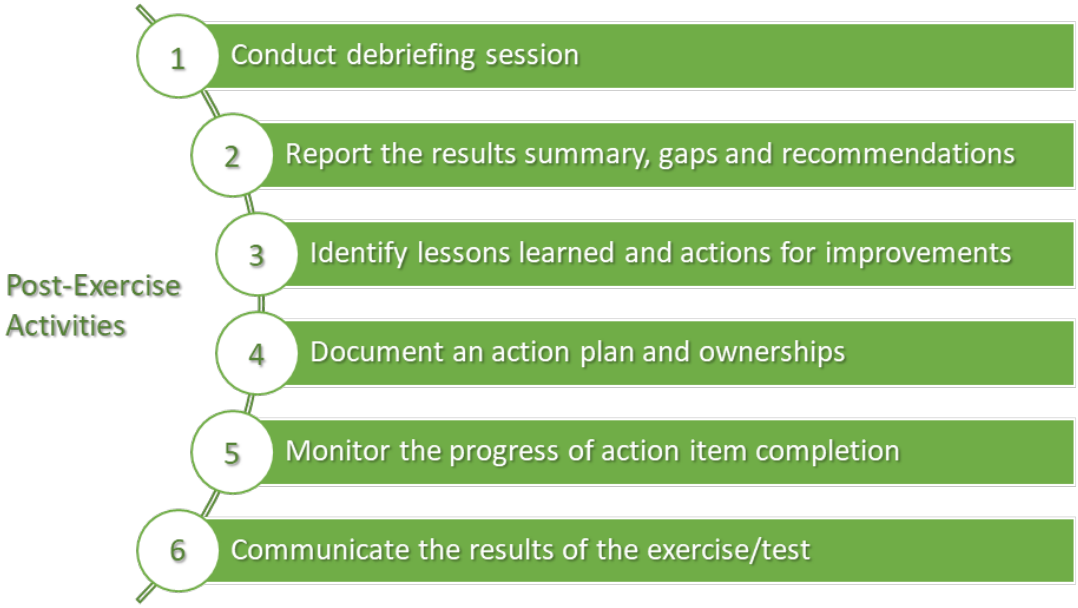
To achieve the objectives outlined above, organizations should focus on the following key elements:

1. **Exercise Planning**: Develop a well-defined exercise program that aligns with the organization's BCM objectives. Determine the scope, objectives, and scenarios for each exercise, involving relevant stakeholders in the planning process.

2. **Exercise Execution**: Conduct various types of exercises, such as tabletop exercises, functional exercises, and full-scale simulations, to test different aspects of the BCM system. Ensure that exercises are realistic, challenging, and follow a controlled approach.



3. **Post-Exercise Evaluation**: After each exercise, conduct a thorough evaluation to identify strengths, weaknesses, and areas for improvement. Encourage participants to provide feedback and insights to refine the BCM system.



4. **Corrective Action and Improvement**: Based on the findings from exercises and assessments, develop and implement corrective actions and improvements to enhance the effectiveness of the BCM system.

This will provide valuable feedback on the processes already mentioned or their results or activities, with the aim of continuous improvement and documentation that is as up-to-date as possible. Affected processes should be for example:

- **Business Impact Analysis (BIA)**: Regularly review and update the BIA to ensure it accurately reflects the organization's critical processes and their dependencies. This information is crucial for developing realistic exercise scenarios.
- **Risk Assessment**: Conduct periodic risk assessments to identify emerging threats and potential disruptions, enabling the organization to adjust its BCM strategy accordingly.
- **Training and Awareness**: Ensure that all employees are adequately trained in the organization's BCM procedures and are aware of their roles and responsibilities during disruptions. Training should be aligned with the results of exercises and assessments.
- **Documentation and Reporting**: Maintain detailed documentation of exercise results, assessment findings, and improvement actions taken. This documentation helps demonstrate compliance, track progress, and support future audits or certifications.
- **Continuous Improvement**: Establish a culture of continuous improvement by integrating lessons learned from exercises and assessments into the organization's BCM system. Encourage ongoing feedback and engagement from stakeholders to drive enhancements.

These activities ensure readiness, identify weaknesses, promote learning, and maintain the relevance of the organization's BCM system. By adhering to the key elements of exercise planning, execution, evaluation, corrective action, BIA, risk assessment, training, documentation, reporting, and continuous improvement, organizations can enhance their resilience and response capabilities. These practices contribute to mitigating the impact of disruptions, safeguarding operations, and maintaining stakeholder confidence in the face of adverse events.

How to Start? Best Practice Approach

In order to establish an effective BCM system aligned with ISO 22301 requirements, organizations should follow a step-by-step approach.
Here are some best practices on how to go forward:

1. **Obtain Top Management Commitment**: Secure commitment from top management to support the implementation of ISO 22301 and allocate necessary resources.
2. **Perform a Gap Analysis**: Identify the organization's current level of compliance with ISO 22301 requirements and determine the project roadmap.
3. **Develop a Project Plan**: Create a comprehensive plan outlining the necessary steps, responsibilities, timelines, and resources for certification.
4. **Formulate a Business Continuity Management Team**: Establish a dedicated team responsible for driving the certification process and ensuring alignment with organizational needs.
5. **Conduct a Business Impact Analysis (BIA)**: Assess critical business processes, dependencies, and potential impacts to guide the development of business continuity strategies.
6. **Establish Business Continuity Policies and Objectives**: Define clear policies and measurable objectives that align with ISO 22301 requirements.
7. **Develop Business Continuity Plans**: Create detailed plans for incident management, crisis communication, IT recovery, and alternative workspace arrangements.
8. **Implement Controls and Measures**: Deploy necessary safeguards, backup systems, redundancy measures, and security protocols to mitigate risks.
9. **Conduct Internal Audits and Reviews**: Regularly evaluate the effectiveness of the BCM system through internal audits, ensuring compliance and identifying areas for improvement.
10. **Train Employees and Raise Awareness**: Provide comprehensive training programs and awareness campaigns to foster a culture of business continuity.
11. **Conduct Mock Drills and Exercises**: Regularly test the BCM system through mock drills and exercises to identify gaps, refine response procedures, and enhance coordination.
12. **Continuously Monitor and Improve**: Establish a system for ongoing monitoring, measurement, and feedback analysis to drive continuous improvement of the BCM system.
13. **Document and Maintain Records**: Maintain accurate and up-to-date documentation of BCM-related activities, supporting compliance and future audits.
14. **Engage External Auditors**: Collaborate with an accredited certification body for the ISO 22301 certification audit, providing access to relevant personnel and documentation.
15. **Foster a Continual Improvement Mindset**: Actively seek feedback, monitor industry trends, and adapt the BCM system to evolving business environments.

Avoid failure – why do BCPs fail?

Business continuity plans can fail due to various reasons, including:

Inadequate risk assessment: Failure to properly identify and assess risks and threats can result in insufficient measures and controls being in place to mitigate them.

Lack of understanding: Insufficient comprehension of the organization, its business operations, critical processes, and dependencies can lead to ineffective BCPs that do not address the specific needs and requirements.

Incomplete or unclear strategies: BCPs that lack well-defined and comprehensive strategies may not provide clear guidance on how to respond to disruptions, resulting in confusion and delays during the recovery process.

Undefined roles and responsibilities: Without clearly identified roles and responsibilities, it becomes challenging to coordinate and execute the necessary actions during a crisis, leading to a lack of accountability and coordination.

Absence of ownership: Without a designated owner or champion for the BCP, there may be a lack of accountability, direction, and ongoing maintenance of the plan.

Missing restoration priorities: Failing to establish a priority list for restoring critical functions and systems can lead to delays and inefficiencies in the recovery process, impacting the organization's ability to resume operations quickly.

Insufficient training: Inadequate training and awareness among employees and stakeholders involved in the BCP can result in a lack of understanding and readiness during a crisis, hindering effective response and recovery efforts.

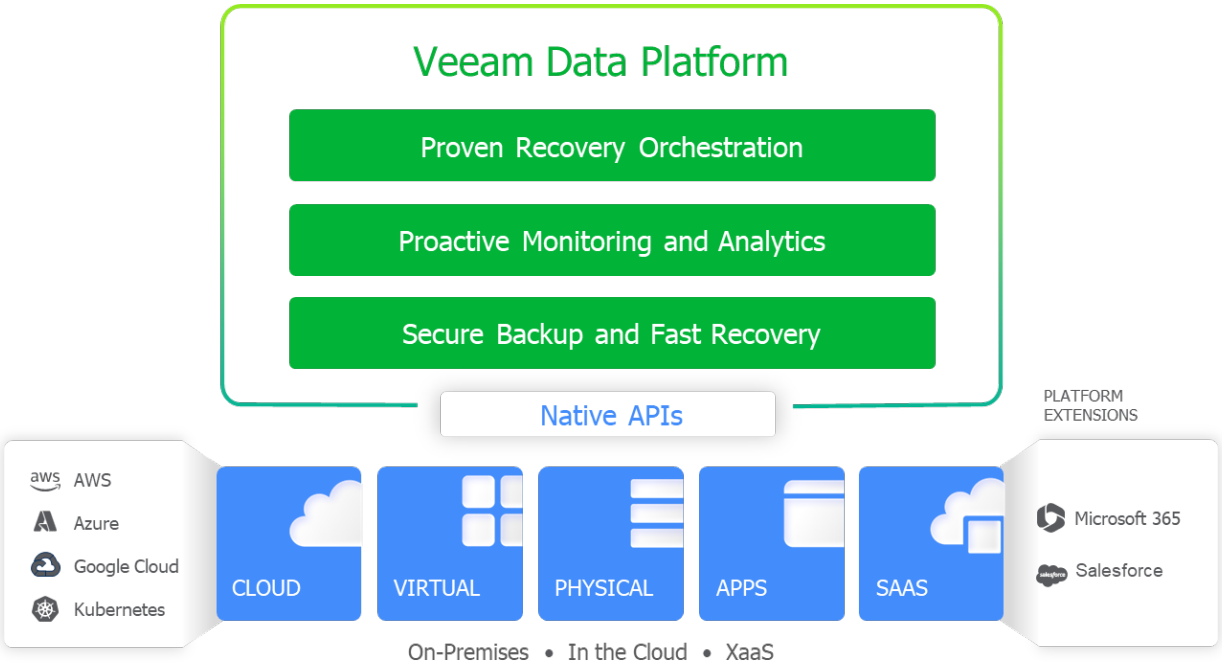
Ineffective data backup and recovery strategies: Inadequate data backup, storage, and recovery mechanisms can compromise the availability and integrity of critical information, undermining the effectiveness of the BCP.

Communication gaps: Without a clear and well-defined communication process, there can be delays, miscommunication, and confusion during a crisis, hindering effective coordination and decision-making.

Lack of testing: Failing to regularly test and exercise the BCP can result in untested assumptions, gaps in the plan, and a lack of confidence in its effectiveness, leaving the organization ill-prepared when an actual disruption occurs.

IV. Veeam Products for IT Disaster Recovery

The Veeam Data Platform is an integrated suite of solutions that empowers organizations to protect, manage, and leverage their data assets effectively. It combines industry-leading backup and recovery capabilities with advanced data management features, such as data orchestration, data governance, and analytics, enabling businesses to optimize data availability, ensure regulatory compliance, and drive intelligent decision-making.
With support for both on-premises and cloud environments, the Veeam Data Platform offers a unified and scalable approach to data protection and management, empowering organizations to unlock the full value of their data while minimizing risk and maximizing operational efficiency.



Overview of Veeam Backup & Replication

Veeam Backup & Replication is a comprehensive data protection and disaster recovery solution designed for virtual, physical, and cloud-based environments.
It is a software suite that offers a wide range of features and capabilities to ensure the availability and recoverability of critical data and applications, with ease of use and enterprise scalability.

Backup and Restore
Veeam Backup & Replication provides efficient and reliable backup for virtual machines (VMs) and physical servers.
It offers image-based backups, allowing application aware processing, reliable and fast recovery, and includes specialized explorers for different applications and platforms, such as Microsoft Exchange, SharePoint, Active

Directory, SQL Server, Oracle, PostgreSQL and more.
These explorers provide granular recovery options, allowing users to restore individual items or application-specific data.

Replication
Veeam offers replication capabilities to create replicas of VMs for disaster recovery purposes. Standard replication provides a very low recovery time objective (RTO), because VM replicas are in a ready-to-start state. For mission-critical VMware VMs where data loss of seconds or minutes is unacceptable, Veeam also provides a CDP replication that features near-zero RPO.
Replicas can be easily tested for failover scenarios, ensuring business continuity and minimizing downtime in case of a disaster.

File-Level Backup
Veeam allows you to back up the files and folders stored on NAS devices (NAS = "network attached storage"). It captures the individual files, maintaining their folder structure and permissions, ensuring the integrity and consistency of the backup. You can schedule regular backups to protect your NAS data and maintain multiple restore points for added flexibility. Veeam uses efficient algorithms and technologies, such as Changed File Tracking (CFT), to optimize backup operations. CFT identifies and transfers only the modified portions of files during subsequent backups, reducing the backup window and minimizing network bandwidth consumption.

Backup copy
Embracing the 3-2-1 rule (in short: *"create 3 copies of your data, store these copies on 2 different media types and move 1 copy off-site"*), Veeam Backup & Replication allows users to create backup copy jobs for offsite and long-term storage. This feature enables the creation of multiple backup copies with different retention policies, optimizing data protection and compliance requirements.

Storage Integration
Veeam integrates with leading storage systems, including Hewlett Packard Enterprise (HPE), NetApp, Dell EMC, and others. This integration provides advanced functionality such as snapshot-based backups, storage-level replication, and direct storage access for enhanced performance.

Instant Recovery
"Instant Recovery" is a Veeam feature that enables users to instantly recover workloads from backup files, reducing downtime and minimizing the impact on business operations. Workloads can be run directly from the backup file while the restore process takes place in the background. Workloads supported for Instant Recovery are complete VMs, virtual disks, physical servers (as VMs), NAS shares as well as databases of MS-SQL or Oracle servers.

Backup Verification
Veeam can ensure validity of the backups by automatically verifying the recoverability of backups and replicas. These features, called SureBackup and SureReplica, involve starting up VMs in an isolated environment, running pre-defined or custom tests to validate the VM integrity and application functionality.

Cloud Mobility
Veeam allows the restore of VMs, physical servers and cloud workloads to public cloud platforms like AWS, Azure, and Google Cloud. This feature simplifies cloud adoption strategies and DR planning.

Direct to Object
Thanks to object storage and cloud-based storage repositories for short-term and long-term retention of backups, Veeam helps optimizing storage costs by optionally using object storage as the primary backup target, or by automatically moving older backups to more cost-effective storage tiers if needed, while maintaining efficient data accessibility.

Data immutability
Backup data generated by Veeam can be protected from ransomware beginning with the first on-prem copy, thanks to the immutability provided by Veeam Hardened Repositories or object storage, leveraging object lock technology.
Data in the cloud, including long-term retention copies either in standard or archive tiers, can be protected, too.

Overview of Veeam One

Veeam ONE is a complete monitoring, reporting, and capacity planning solution designed to provide visibility and insights into virtual, physical, and cloud-based IT environments. It works in conjunction with Veeam Backup & Replication to offer a complete data protection and management solution.
It helps IT administrators optimize resources, proactively identify, and resolve issues, and gain valuable insights into the performance and health of their infrastructure.

Monitoring and Alerting
Veeam ONE offers real-time monitoring of the virtualization environment, including virtual machines, hosts, storage, and the Veeam backup infrastructure. It provides proactive monitoring and alerting capabilities, allowing detection and resolution of issues before they impact the production environment.

Dashboards and Reporting: Veeam ONE offers customizable dashboards and reports to provide a consolidated view of the infrastructure. It includes pre-built templates and allows you to create custom reports to track key performance indicators, capacity trends, backup and replication status, and more. It enables to identify inefficiencies, allocate resources effectively and plan for future growth, and provides recommendations for optimization and best practices, helping enhance the performance and stability of your environment.

Business View: Veeam ONE enables you to categorize your virtual infrastructure based on business units, departments, or any other custom-defined criteria. This feature provides a business-centric view of your environment, allowing you to understand resource allocation and costs in relation to specific business units or applications.

Automation and API Integration: Veeam ONE offers automation capabilities through PowerShell and RESTful API. This enables integration with third-party systems and the automation of monitoring, reporting, and data protection tasks, enhancing operational efficiency.

Overview of Veeam Recovery Orchestrator

Veeam Recovery Orchestrator (VRO) is a disaster recovery orchestration solution designed to simplify and automate the recovery process for virtual and physical workloads. It helps organizations plan, test, and execute

disaster recovery scenarios to ensure business continuity in the face of disruptions and simplifies the documentation process for compliance and audit.

VRO seamlessly integrates with Veeam Backup & Replication, leveraging its capabilities. It utilizes Veeam's image-based backups, replicas, and storage integrations to streamline and automate the recovery process for virtual and physical workloads, enabling organizations to achieve their business continuity objectives by minimizing downtime and ensuring rapid recovery.

As Veeam Recovery Orchestrator is the most powerful tool in the Business Continuity/Disaster Recovery framework, it will be discussed in more detail in the following sections.

V. IT Disaster Recovery Planning with Veeam

Introduction

Importance of IT Disaster Recovery Planning with Veeam

Data is a crucial asset for organizations, and a disaster disrupting data integrity and availability can have severe consequences: financial or reputational loss, legal/regulatory impact, and in the worst case involve human lives. Veeam Backup & Replication provides efficient backup and replication, keeping data safe with multiple copies, while Veeam Recovery Orchestrator is the solution that allows quick recovery of critical systems and applications, minimizing downtime and allowing business to continue operations without significant disruptions.

The ability to quickly restore systems and applications ensures that revenue generation and customer service can resume promptly, mitigating potential revenue losses; it helps organizations adhere to regulatory standards, ensuring that critical data is protected and recoverable as per legal obligations; besides, it demonstrates the commitment to business continuity and data security that, in turn, fosters trust among customers, partners, and stakeholders.

Lastly, having a well-defined disaster recovery plan in place with Veeam provides peace of mind to organizations. It reassures that in the event of a disaster, the necessary steps and procedures are in position to swiftly recover critical systems and data, minimizing the overall impact on operations and reputation.

Key Benefits of IT Disaster Recovery Planning with Veeam

Veeam Recovery Orchestrator provides the following key features for IT disaster recovery planning:

Recovery Plan Orchestration

Veeam Recovery Orchestrator allows to create recovery plans that define the order and dependencies of virtual

and physical machines during the recovery process. It provides a visual interface to design the recovery workflow, ensuring the proper sequencing of actions and resource allocation.
The customization allows to define recovery steps, actions, and dependencies to ensure the optimal recovery of the workloads.

Plan Readiness Check
The readiness check is a feature that allows organizations to assess the readiness of their infrastructure for successful disaster recovery. The readiness check helps identify any potential issues or inconsistencies in the environment that could impact the recovery process, running at scheduled times infrastructure assessments, dependency analysis, validation of backup jobs and more. It is a very low-impact and fast method to confirm that configuration of an orchestration plan matches the DR environment, and that all prerequisites are in place (e.g. access permissions, restore points, VM replicas, storage systems – basically plan 'metadata' which is not very impactful but important for successful plan execution). Therefore, it is good practice to run these readiness checks on a regular schedule, e.g. daily. With Veeam Recovery Orchestrator, you can schedule and fully automate this process and it provides a very detailed "readiness check report" after each run, including a simple "success/warning/failed" summary at the top to quickly identify the overall status of your orchestration plans.

Non-Disruptive Testing
Veeam Recovery Orchestrator enables testing of the recovery plans without impacting production environments. Leveraging Veeam Backup & Replication's Virtual Labs, called DataLabs in VRO, it provides isolated environments for testing and allows to validate the recoverability of workloads and applications.

Automated Documentation
The solution also generates documentation for recovery plans, outlining the recovery steps, actions, and dependencies defined in the recovery plan.
By automatically documenting the recovery workflow, VRO helps organizations meet compliance requirements by providing clear and auditable records of their disaster recovery capabilities. It simplifies the documentation process, saving time and effort that would otherwise be required to manually create and maintain detailed recovery plan documentation. This documentation serves as a comprehensive record of the disaster recovery procedures and can be used for compliance, auditing, and reference purposes.

Automated Failover and Failback
Veeam Recovery Orchestrator automates the execution of failover and failback operations. It orchestrates the recovery process, ensuring that virtual and physical machines are brought online in the correct order and that dependencies are resolved automatically.
When a disaster occurs and the decision to initiate fail over has been made, Veeam Recovery Orchestrator automates the failover process, ensuring the orchestrated execution of recovery plans. It coordinates and executes a series of actions required for a successful recovery, that may include powering on virtual machines, establishing network connectivity, configuring IP addresses, and mounting storage volumes and so on. The orchestration ensures that the recovery process progresses smoothly, adhering to the defined recovery plans.
Once the disaster situation has been resolved and the production environment is available, Veeam Recovery Orchestrator also allows to automate the failback process. Failback involves returning the recovered virtual and physical machines from the recovery environment to their original production location, ensuring that any changes or updates made during the failover period are synchronized back to the production environment without causing conflicts or data loss.

High Level Step-by-Step Guide to IT DR Planning with Veeam

1. Recovery Strategies

Developing recovery strategies based on the risk assessment and business impact analysis

When developing recovery strategies for IT disaster planning, it is essential to base them on a thorough risk assessment and business impact analysis. This ensures that the strategies are aligned with the specific needs and priorities of the organization.

The customer should run a risk assessment, identifying the potential risks that could disrupt IT systems and operations, evaluating the likelihood of each identified risk occurring and determining the potential impact of each risk. These risks can include natural disasters, cyberattacks, hardware failures, power outages, and human errors.

Most importantly, the customer should identify systems and applications that are vital for the organization's day-to-day operations and revenue generation, and prioritize them. These may include customer databases, e-commerce platforms, communication systems, and core business applications.

The customer should assess the maximum acceptable downtime and data loss limits for each critical system and application, defining Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

For each critical system or application, the customer should evaluate the financial and operational impact of a disruption, considering factors such as revenue loss, productivity impact, customer dissatisfaction, contractual obligations, and regulatory compliance.

Based on this information, the customer will define the recovery priorities for each critical system and application, assigning recovery levels or tiers to determine the order in which systems should be restored.

Veeam partners and consultants as well as Veeam representatives (e.g. technical sales or technical account managers) can support into choosing the appropriate recovery methods, based on the RTOs and RPOs determined earlier. Options may include backup and restore, failover to alternate sites, cloud-based recovery, or a combination of these approaches.

A high-level procedure for executing the selected recovery methods should be created, along with prerequisites for the recovery process, restore data and systems location, and information on how to validate the recovered environment. This information will help Veeam to identify the appropriate Veeam solution and configuration for each recovery strategy.

Identifying appropriate Veeam products and solutions for each recovery strategy

Veeam Backup & Replication is a complete solution, providing all the necessary features to implement any recovery plan. It offers the functionality required to achieve the target RPO/RTO, ensuring data is either backed up in a suitable repository or replicated in the secondary site.

The following table depicts how different data protection technologies compare in terms of RPO, RTO, cost and effectiveness:

	Tape Backup	Deduplication Appliance	Standard Disk On-Prem S3	Cloud Storage	Replication	CDP-Replication
Tier Type	Cold (Offline)	Cold-Hot	Hot	Hot	Hot	Live
Recovery Type	Restore	Restore	Restore	Restore	Power-on	Power-on
RPO	Hours	Hours	Hours	Hours	Minutes/Hours	Seconds
RTO	Days	Hours/Days	Hours	Hours/Days	Minutes/Hours	Minutes/Hours
COST per TB	Low	Moderate/Low	Moderate/High	High	High	High
Protection from Disaster	Yes	Yes	Yes	Yes	Yes	Yes
Protection from Ransomware Attack	Yes	Yes	Yes	Yes	No *	No *
* except when more Restore Points are kept						

- **Tape** is the coldest tier, cheaper and reliable but very slow to restore; Secure Restore is not possible, so in case of ransomware attack manual activity is required to check the VMs for malware. Tapes in DR scenarios should only be considered as the last resort.
- **Deduplication appliances** have exceptional write performance and can considerably reduce the size on disk and in site-to-site replication, keeping costs per TB low. The drawback is that restores require data to be rehydrated (rebuilt from deduplication), which is typically slower than traditional repositories. They don't perform well with random I/Os, so Instant Recovery cannot be used, extending expected RTOs. Depending on the vendor and model of the deduplication appliance, immutability may be available, and Secure Restore can be used in case of ransomware attack, however with reduced performance.
  Please note that some deduplication appliances store fresh data in hi-performing "landing zones", while the long term retention is in the colder tier with deduplication. In this case, the same considerations as standard repositories can be applied.
- **Standard disk and on-prem S3 repositories**, like Veeam Hardened Linux Repository or any S3 compatible Object Storage system, provide a good compromise between cost and RTO, enabling the use of Instant Recovery technology to bring up essential services as soon as possible, but relying on restore procedures for other workloads. Backup immutability ensures that even in the case of a ransomware attack the backup data can be restored from a previous restore point. Additionally, Secure Restore allows to scan for malware that might already exist in the backup data before recovering from it, avoiding to re-introduce the malware into production.
- **Cloud Storage** represents a very heterogeneous offering in the market, relying on a large number of vendors to provide this kind of service. The features may be almost the same as an on-prem object storage, however similar if not far-reaching costs can be considered on average because of extra transfer cost and/or transaction fees to be added to the bill. The RTO can also be higher, because, depending on circumstances, vendor throttling can occur to decrease throughput, and in any case the maximum achievable depends on the bandwidth available. Backup immutability may be offered from vendors offering a compatible service, including but not limited to Microsoft Azure and Amazon S3.
- **Replication**, in both standard and CDP types, can guarantee the lowest RTO and RPO but is potentially more expensive, since replicated data takes capacity on the target primary datastore with a higher per TB price as usual backup storage.
  In case of a ransomware attack, the replica will contain the same corrupted data as the primary

environment, making replication based recovery not ideal in this scenario. However, Veeam Backup and Replication allows to store additional Restore Points for both standard and CDP replication, so it may still be possible to restore a clean point of the VM. However, a malware scan will need to be run manually in an isolated environment. Please note that storing more points means increasing the storage usage, and therefore higher costs.

Another approach would be to select a Veeam based strategy by reviewing the scenarios identified by the risk analysis and evaluate which kind of Veeam protection will be able to cover those. An easy example might look like this:

Protection type / target storage	Scenarios						
	User file deleted / corrupted	VM deleted / corrupted	physical Server HW failure/corruption	VM source storage unavailable	Primary data center outage	Typical ransomware attack	Insider attack with physical access
Backup *local*	Y	Y	Y	Y	N	N	N
Backup Copy *offsite*	Y	Y	Y	Y	Y	N	N
Replication *offsite*	Y	Y	N/A	Y	Y	N	N
CDP *offsite*	Y	Y	N/A	Y	Y	N	N
Backup on Hardened Repository *local + immutable*	Y	Y	Y	Y	Y	Y	N
Backup to Tape *offline*	Y	Y	Y	Y	Y	Y	N
Backup to Object Storage *local*	Y	Y	Y	Y	Y	N	N
Backup to Object Storage *local + immutable*	Y	Y	Y	Y	Y	Y	N
Backup to Object Storage *offsite + immutable*	Y	Y	Y	Y	Y	Y	Y

Y	Risk is covered
N	Risk is not covered
N/A	not applicable

Note: This illustration is just a generic example of how such an approach could look like. It is by no means trying to provide a complete list of the possible risk scenarios or the available protection options (or combinations of those) you can achieve using Veeam Backup & Replication.

While Veeam Backup and Replication provides all the functionality needed to manage data recovery in the event of a disaster, it requires creation of plan documentation by hand, and manual management of testing procedures and actual disasters.
Veeam Recovery Orchestrator provides orchestration and automation of all aspects of a recovery plan and therefore it is strongly recommended, after the identification of the most appropriate technologies for the recovery plans.

Documenting recovery strategies for each business process and application

In a disaster recovery scenario, managing the recovery of different business applications involves creating multiple recovery plans and grouping together related workloads. This approach ensures that interconnected components, such as web servers, application servers, database servers and so on, are recovered together to maintain application functionality.

- **Application Dependencies**: as a first step, the dependencies between different business applications and their associated VMs should be identified, determining which VMs need to be recovered together to ensure proper functionality.
- **Group Workloads**: a recovery group should be documented, grouping together VMs that have interdependencies. Each recovery group should include the VMs required for a specific business application or a subset of applications with related functionalities.
- **Recovery Priorities**: recovery priorities must be determined for each recovery group, based on business impact analysis and the criticality of the applications. Recovery levels or tiers should be assigned, to prioritize the order in which recovery groups should be restored.
- **Recovery Type**: depending on the criticality of the application, establish which kind of recovery type will be used for each recovery group, between backup/restore and replication, taking into account target RPO, RTO and cost. Instant Recovery should be considered for workloads that need a rapid recovery as an interim solution before or during the broader recovery of multiple, inter-dependent workloads.

Documenting the recovery strategy for each business process and application will help define Veeam Recovery Orchestrator recovery plans and their configuration.

2. Plan Development

Developing a comprehensive IT Disaster Recovery Plan
Next to the definition and documentation of the recovery strategy, the detailed recovery plans are created in Veeam Recovery Orchestrator.

Multiple recovery plans can be created based on the grouped workloads, to ensure services are restored in the correct order. Within each recovery plan, it is necessary to specify the recovery steps required to restore the associated workloads, and define the sequence of actions, such as powering on VMs, restoring data from backups or replicas, and configuring networking settings and so on.
It is important to determine the execution order of the recovery plans based on their recovery priorities, and any specific dependencies between them to maintain application integrity.

After the creation of the recovery plans, regular testing and validation should be performed to ensure their effectiveness. Veeam Recovery Orchestrator provides non-disruptive testing capabilities using DataLabs, to validate the recovery process without impacting production systems and verify that the recovery groups are restored together successfully, and the applications function as expected.

The plan documentation is the last part but not less important. The recovery plans, including the grouped workloads, recovery steps, and execution order, are automatically documented by Veeam Recovery Orchestrator. The relevant IT teams and business units should have access to the documentation and be aware of their roles and responsibilities during the recovery process.
Keep in mind that recovery plans should be regularly reviewed and updated, to incorporate any changes in application dependencies, workloads, or business requirements. Automated documentation is based on editable templates that can be enriched with additional, static information e.g., important contact details

(internal/external), building access information, communication plans – basically all information that is required to initiate execution of a recovery plan, but which is not directly available to Veeam Recovery Orchestrator.

As BCP documentation is a crucial part of the overall BCMS, it is a huge benefit to have a large portion of the documentation being created automatically by Veeam Recovery Orchestrator – a reason why this feature should not be underestimated!

Documenting the roles and responsibilities of the IT Disaster Recovery team

Veeam Recovery Orchestrator includes the concepts of Roles and Scopes to define and manage roles and responsibilities within the disaster recovery planning process. These concepts align with the roles and responsibilities described in the ISO 22301 model, which is a standard for business continuity management. There are three roles available: Administrator, Plan Author, and Plan Operator:

- **Administrator**: this role has full control and access rights over the solution. Administrators are responsible for managing the Orchestrator server, configuring settings, managing users, and overseeing the disaster recovery planning process.
  This role aligns with the role of a Business Continuity Manager in the ISO 22301 model. The Business Continuity Manager has overall responsibility for the development, implementation, and maintenance of the business continuity management system.

- **Plan Author**: this role is responsible for creating and designing recovery plans within Veeam Recovery Orchestrator. Plan Authors define the sequence of recovery steps, specify dependencies between virtual machines, and configure advanced recovery options, and collaborate with other stakeholders to gather information and design effective recovery strategies.
  This role aligns with the role of a Recovery Planner or Recovery Coordinator in the ISO 22301 model. These individuals are responsible for developing and maintaining recovery plans and coordinating recovery activities.

- **Plan Operator**: this role executes recovery plans created by Plan Authors. Plan Operators are responsible for initiating the recovery process, monitoring progress, and ensuring that the recovery plan is executed successfully. They coordinate with IT teams, follow predefined recovery procedures, and troubleshoot any issues that may arise during the execution. Additionally, Plan Operators are also responsible of the plan testing, that can be either run manually, or scheduled to run unattended.
  This role aligns with the role of a Recovery Team Member or Recovery Coordinator in the ISO 22301 model. They are responsible for implementing the recovery plans and managing the recovery operations.

Access	Administrator	Plan Author	Plan Operator
Administration	Full	None	None
Create, Edit, Enable, Disable, Reset, Delete Plans	Full	Full	Reset only
Check Plans	Full	Full	Full
Test Plans	Full	Full	Enabled plans only
Schedule and Run Plans	Full	None	Enabled plans only

Reports and Templates	Full	Full	Full

Veeam Recovery Orchestrator also provide Scopes, in order to grant more granular permissions to users managing resources within the solution. Scopes allow administrators to restrict user access to specific resources or recovery plans, ensuring that users have appropriate permissions based on their roles and responsibilities. Only users assigned with Plan Author and Plan Operator roles can be added to a scope.

Defining the steps and procedures for each recovery strategy

The recovery of workloads with Veeam Recovery Orchestrator potentially involves the coordination of different operation types, such as restore from backup, replica failover, storage failover, and cloud failover, each with their respective recovery plans.
Most recovery plans will require the definition a Recovery Location, consisting of groups of resources used as target locations; they vary according to the failover type, as each has its own characteristics and requirements which we can breakdown as follows:

Restore from Backup: Restore plans

Restore from Backup involves using Veeam backups as the source for recovering workloads. It requires to have backup copies stored in a Veeam backup repository in the DR site and allows to restore VMs and physical machines from backup files in case the primary production environment becomes unavailable or compromised from ransomware.
In Veeam Recovery Orchestrator, restore from backup is implemented through Restore Plans: the configuration of the plan requires to define a Restore Recovery Location to which workload groups included in the plan will be restored, that consists of compute and storage resources in a vSphere environment. The Recovery Location can also be configured to enable Instant VM Recovery, to ensure a lower RTO for critical workloads.
The plan also allows to customize the recovery process by adding additional Steps, which typically include starting/stopping services, executing scripts, and verifying the status of services.
Restore plans provide the option to automatically start protecting the VMs in the plan after the recovery, with a backup or replication job.

Replica Failover: Replica plans

Replica failover relies on Veeam replicas, which are copies of VMs created and maintained in a separate location. Replicas can be configured as standard or CDP and offer near-instant recovery and minimal data loss in case of a disaster.
In Veeam Recovery Orchestrator, replica failover is implemented through Replica Plans and CDP Replica Plans: the configuration of the plans is very similar, and since the Replica VM is already on the target infrastructure, they don't require to define any Recovery Location.
The plan also allows to customize the recovery process by adding additional Steps, which typically include starting/stopping services, executing scripts, and verifying the status of services.
The only difference between a Replica and a CDP Replica Plan is that only Replica Plans provide the option to automatically start protecting VMs in the plan after the recovery, with a backup or replication job.

Storage Failover: Storage plans

Storage failover leverages storage-based replication technologies of storage systems to enable rapid recovery of workloads and involves redirecting storage access to a secondary storage system in case a disaster strikes.

To perform storage failover, supported storage systems with volume replication capabilities, such as NetApp ONTAP or HPE Primera (3PAR), are required. The storage systems should be properly configured and synchronized, and it's recommended that the creation and transfer of storage snapshots is driven using Veeam Backup & Replication, allowing for seamless failover and failback operations.

In Veeam Recovery Orchestrator, storage failover is implemented through Storage Plans: the configuration allows to add inventory groups that relate to datastores protected by storage replication and datastores backed by storage systems added to Orchestrator.

The plan also allows to customize the recovery process by adding additional Steps, which typically include starting/stopping services, executing scripts and verifying the status of services.

When Storage Plans are executed, it's possible to configure a trigger that will automatically reverse the replication to re-protect volumes included in the plan, allowing to fail back to the production location very quickly.

Restore to Cloud: Cloud plans

Restore to cloud enables the recovery of workloads to an Azure cloud environment. It offers flexibility and scalability in disaster recovery scenarios and enables cloud-to-cloud DR using Veeam Agents for cloud workloads.

In Veeam Recovery Orchestrator, restore to cloud is implemented through Cloud Plans: the configuration of the plan requires to define a Cloud Recovery Location to which workload groups included in the plan will be restored, and it consists of a Microsoft Azure compute account, registered in the Veeam Backup & Replication server that is connected to Veeam Recovery Orchestrator.

The target repository for backups can be in any location external to the primary site: inside Azure in a blob storage (possibly in the same region as the Recovery Location to avoid additional cost) or in any other service provider object storage (though additional egress charges may occur).

The plan also allows to customize the recovery process by adding additional Steps, which mainly include VM Power actions and the ability to run custom scripts.

Testing the IT Disaster Recovery Plan

In Veeam Recovery Orchestrator, testing methodology plays a crucial role in ensuring the readiness and effectiveness of disaster recovery plans. The solution provides several testing capabilities, and the basics are verified with the readiness check: depending on the types of plan, it helps identify any potential issues or gaps in the recovery plans before an actual disaster occurs; it provides confidence in the recoverability of workloads and ensure that the necessary resources and dependencies are in place for successful recovery.

Readiness checks should be scheduled and run frequently, at least weekly; this ensures organizations can proactively address any issues, fine-tune recovery plans, and maintain the readiness of their disaster recovery strategy.

Their main focus is to ensure the availability of critical systems like Veeam Backup & Replication server, VMware vCenter, and storage systems. However, the specific verifications performed vary depending on the type of plan being executed:

Backup Plans

When testing backup plans, Veeam Recovery Orchestrator verifies the availability and recoverability of

backups. It checks if the required backups are available and if they can be successfully restored within the recovery point objectives (RPOs).

Replica and CDP Replica Plans
Readiness checks for replica plans focus on validating the replication process. Veeam Recovery Orchestrator ensures that replicas are up to date, consistent, and ready for failover. It verifies the replication status, connectivity between source and target environments, and the ability to power on and operate replica VMs.

Storage Plans
For storage plans, readiness checks primarily involve validating the connectivity and accessibility of the storage infrastructure. Veeam Recovery Orchestrator ensures that the storage resources required for recovery are accessible, functioning correctly, and ready for use.

Cloud Plans
Readiness checks for cloud plans verify the connectivity to the cloud provider, assess the availability of the required cloud resources, and validate the deployment and configuration of the necessary infrastructure.

Veeam Recovery Orchestrator can use a DataLab to test the entire plan, including the verification of vSphere and agent backups, replicas and storage snapshots. DataLabs are based on Veeam Backup & Replication Virtual Labs, and allow testing in an isolated environment, separate from production. This environment mimics the production setup and allows for thorough testing without risking the live systems, ensuring that critical applications and services remain unaffected while validating the recovery plans.
All changes made to machines during a DataLab session will be discarded as soon as the testing process is over.

Testing is currently not supported for cloud plans.

3. Plan Implementation

Implementing the IT Disaster Recovery Plan
In Veeam Recovery Orchestrator, the recovery plan implementation involves defining steps that will be executed during the pre-plan, plan, and post-plan phase. These shape the orchestration of the recovery process and ensure the plan includes all actions necessary for proper recovery.

Pre-plan steps are executed before the actual recovery plan is initiated. These steps are designed to prepare the environment and ensure that all prerequisites for successful recovery are in place. This can also include custom scripts or email notifications etc., basically any extra steps that involve other parts of the greater BCP in the organization.

Pre-plan steps may include activities such as stopping certain services or processes, taking a pre-recovery snapshot or backup, syncing the replica to the latest state, allocating necessary resources or perform any reconfiguration on

the recovery site. Custom scripts can also be prepared in advance and run at this step: their use may potentially be required to activate external systems needed for the organization to operate properly.

The purpose of pre-plan steps is to create an optimal starting point for the recovery process, minimize potential conflicts, and streamline the recovery operations.

Plan steps are the core components of a recovery plan in VRO. They define the sequence of actions to be performed during the recovery process, and can include various operations, such as restoring from backup or powering on virtual machines, executing scripts or commands, and configuring network settings.

Each plan step represents a specific actions or task required to restore or resume critical services and is defined based on the recovery objectives and dependencies of the applications and systems involved.

Post-plan steps are executed after the main recovery steps; these steps focus on post-recovery activities required to validate the successful restoration of services and ensure the continuity of operations.

Post-plan steps can involve tasks such as performing validation tests: monitoring the recovered environment, verifying application functionality, and notifying stakeholders about the recovery completion. Custom scripts are also likely to be run at this step as well, to trigger external systems after the application has been recovered.

These steps help confirm that the recovery process has been completed successfully and that the recovered systems are functioning as expected. Depending on the type of recovery or the importance of the recovered services, it is most likely required to enable backup of the recovered systems which are now the 'new' productive systems, hence they need the same protection as before recovery plan execution. Post-plan steps help to automate the configuration of these backups as well.

Training the IT Disaster Recovery Team

During the recovery planning, it is essential to advise the customer to carefully consider the choice of operators who will be responsible for running the recovery plans in Veeam Recovery Orchestrator, so the roles within can be configured and appropriate permissions and responsibilities to team members are assigned.

Selecting operators for running the recovery plans involves identifying individuals with the necessary knowledge, skills, and expertise in IT disaster recovery procedures. Operators should have a solid understanding of the organization's infrastructure, applications, and dependencies to effectively execute the recovery plans.
Generally speaking, operators should have undergone training and have practical experience in disaster recovery scenarios and in the use of Veeam Recovery Orchestrator.
It is beneficial to have a mix of team members who are familiar with different systems, applications, and platforms to cover a wide range of recovery scenarios.

Veeam Recovery Orchestrator provides role-based access control to manage user permissions and responsibilities within the solution, and the Plan Operator role should be assigned to operators who will execute the recovery plans: they initiate the recovery process, monitor progress, and ensure successful execution.
During the configuration of VRO roles, it's important to assign permissions that align with the specific

responsibilities of each team member, to ensure appropriate access to perform tasks without having more privileges than required.

Reviewing and Updating the Plan Regularly

As detailed previously, readiness checks assess the health and functionality of the recovery plans and should be run on a consistent basis. Regular checks ensure that the required resources, dependencies, and configurations are up to date, and that the recovery plan will succeed in case a disaster occurs.
In addition to scheduled checks, it is crucial to perform manual runs whenever there are changes in the IT infrastructure, especially in critical systems. This includes modifications to virtual machines, applications, storage systems, networks, or any other components that are part of your recovery plans. Manual runs validate the recovery process against the latest changes, ensuring plans remain accurate and reliable.
Should errors occur, the plan should be reviewed and adjusted as soon as possible to avoid being exposed with no protection from disaster. The documentation automatically produced by VRO supports the troubleshooting by providing complete information about the plan run, including possible causes and remediations on warnings and errors.

The plan documentation generated by Veeam Recovery Orchestrator (plan definitions, reports, test results, etc) should be saved in a safe place, easily accessible by the BCP team, and regular backups of this location should be made. This backup data should be considered as critical, and compliant with the 3-2-1-1-0 rule for maximum protection and resiliency.

VI. Best Practices for Business Continuity Planning with Veeam

1. Involving Key Stakeholders

Collaborating with business leaders to identify critical business processes and applications
Engage with business leaders to understand critical operations and applications that are vital for the organization's continuity.
Evaluate existing disaster recovery plans and methodologies to identify areas for improvement. Provide expert guidance and recommendations to enhance the effectiveness, efficiency, and resilience of the plans.

Engaging IT teams to develop and implement the IT Disaster Recovery Plan
Collaborate with IT teams to create a comprehensive IT Disaster Recovery Plan, involving key stakeholders to gather requirements, assess risks, and design recovery strategies.
Provide ongoing support to IT teams in reviewing and validating the recovery plans, and help ensure that the plans are accurate, up to date, and aligned with the organization's objectives. Offer guidance and expertise to address any gaps or improvements needed to enhance the correctness and reliability of the recovery plans.

2. Testing the Plan Regularly

Conducting regular testing of the IT Disaster Recovery Plan
Assist in creating test plans that simulate disaster scenarios and include steps to validate the recovery process. Support the utilization of DataLabs, or the execution of failover/failback procedures to test the recovery plan in a controlled environment. This helps identify any potential issues, refine the plan, and ensure the organization's ability to recover critical systems and data.

Leverage the documentation of the testing process
Assess the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) achieved during testing and actual recovery scenarios using the documentation generated by Veeam Recovery Orchestrator for these operations. Use this information to refine and optimize the DR plans, ensuring they align with the organization's desired recovery objectives and minimize downtime in case of a disaster.

3. Maintaining Documentation

Documenting all aspects of the IT Disaster Recovery Plan

Support the creation of high-level documentation that covers various aspects of the IT Disaster Recovery Plan, such as risk assessment, business impact analysis, recovery strategies, and plan development. This documentation serves as a reference and guide for effective disaster recovery operations, and as a basis to create Veeam Recovery Orchestrator Recovery Plans.

Ensuring that documentation is up-to-date and easily accessible

Advise to regularly update the documentation to reflect any changes in the IT infrastructure, applications, or recovery strategies. The documentation, along with the detailed reports produced by Veeam Recovery Orchestrator, should be easily accessible to the relevant stakeholders, ensuring they have the most current and accurate information readily available.

Backing up the documentation regularly

Implement a regular backup process to safeguard the documentation from any potential data loss or system failures. Advise using Veeam to regularly create backups of the documentation and store them in secure locations, ensuring its availability even in the event of an unforeseen disaster or technical issue.

VII. Conclusion

Recap of key takeaways for IT Disaster Recovery Planning with Veeam

- Engage with business leaders to identify critical processes and applications.
- Collaborate with IT teams to develop and implement the IT Disaster Recovery Plan.
- Conduct regular testing of the plan to ensure its effectiveness and readiness.
- Make the best use of Veeam documentation to review and improve the DR plans based on achieved RPO and RTO.
- Support documentation of all aspects of the plan, including risk assessment, business impact analysis, recovery strategies, and plan development.
- Advise documentation must be up-to-date, easily accessible, and regularly backed up.
- Recognize the importance of continuous improvement and maintenance of the IT Disaster Recovery Plan.

- Regularly review, update, and refine the plan to address changing business needs, IT infrastructure, and industry best practices.

Importance of continuous improvement and maintenance of the IT DR Plan

Disaster Recovery Plans should be reviewed and updated regularly, so organizations can adapt to evolving business needs, technological advancements, and emerging threats. This proactive approach helps to optimize the recovery strategies and enhance the organization's ability to respond to and recover from disasters.
Continuous maintenance – as described in the ISO 22301 business continuity planning lifecycle – ensures that the plans remain up to date, aligned with industry best practices, and capable of effectively safeguarding critical systems and data.

In conclusion, Veeam provides the essential tools and capabilities to help organizations meet the goals of Business Continuity and Disaster Recovery, through the adherence to the ISO 22301 standard.
With Veeam, you can confidently protect your data, ensure business continuity, and achieve resilience in the face of any challenge.