

HPE Cybersecurity Services

Cyber Resilience

Cyber threats are increasing in both frequency and sophistication, disrupting operations, compromising data, and exposing organizations to regulatory and financial risk. Prevention alone is no longer sufficient. A comprehensive cyber resilience strategy—integrating cybersecurity, disaster recovery, and business continuity—is essential to ensure rapid recovery, maintain operations, protect reputation, and meet compliance obligations.

Effective cyber resilience requires coordinated orchestration across cybersecurity, crisis management, business continuity, and disaster recovery. While market offerings often emphasize recovery, HPE takes a holistic approach that covers planning, preparation, prevention, detection, response and recovery. Successful outcomes depend on unified governance, clearly defined roles, repeatable playbooks, continuous monitoring, and resilient architectures that enable rapid restoration with minimal disruption. HPE combines people, processes, and technology to align stakeholders, automate recovery, validate readiness, and accelerate time-to-value.

HPE Cybersecurity Services - Cyber Resilience offerings are organized into multiple journeys that span the disciplines needed for transformation. Each journey is supported by a set of modular services that can be combined to build a tailored cyber resilience program. To help organizations understand the multidimensional approach and prioritize a transformation program across these journeys, HPE offers a Cyber Resilience Advisory Workshop.

Journeys and service modules

Cyber Resilience Readiness journey

- Cyber Resilience Readiness Assessment
- Cyber Resilience Tabletop Exercise
- Cyber Incident Response Plan Development
- Cyber Resilience Program Plan and Development

Disaster Recovery Modernization journey

- Business Impact Analysis
- Disaster Recovery Capability Maturity Analysis
- Disaster Recovery Plan Refresh

Business Continuity Management Evolution journey

- Business Continuity Maturity Assessment
- Risk Assessment for Business Continuity
- Business Continuity Plan Refresh (Scenario Development)

The Business Continuity Management Evolution journey can be extended through additional capabilities such as Business Continuity Management Automation and Business Continuity Management Advisory Office, under the guidance of HPE Consultants.

Cyber Resilience Advisory Workshop

Service overview

Gain an end-to-end understanding of the multidimensional cyber resilience problem and quickly identify where your organization sits in cyber resilience maturity. The workshop surfaces gaps across people, processes, and technology so stakeholders can choose the most impactful journey to prioritize: Cyber Resilience (CR) Readiness, Disaster Recovery (DR) Modernization, or Business Continuity Management (BCM) Evolution.

Designed for both technical and non-technical participants, the session aligns executive, IT, security, and operational stakeholders. Through short briefings, real-world ransomware scenarios, and guided assessment questions, we map current posture, highlight immediate risks, and pinpoint high-value controls and processes to reduce exposure and recovery time.

Service benefits

- Provides a clear, shared view of cyber resilience definition and concepts.
- Help in the identification of priority pain points and potential project paths (CR, DR, BCM).
- Discusses defensive controls and strategy for improving cyber resilience
- Shortlist of critical controls and testing needs to validate resilience assumptions.

Service feature highlights

- Interactive Workshop led by HPE experts and consultants
- Provides an end-to-end view of multidimensional cyber resilience and shows where your organization sits in resilience maturity.
- Surface gaps across people, processes, and technology to help prioritize Cybersecurity practice, DR readiness, or BCM modernization.
- Designed for both technical and non-technical participants, aligning executives, IT, security, and operations through real-world ransomware scenario and guided assessments.
- Cross-functional engagement session that includes executives, IT, security, and operations to align resilience goals and obtain stakeholder buy-in.
- Guided assessment using real-world ransomware scenario across people, processes, and technology that produces prioritized journeys (CR readiness, DR modernization, or BCM evolution)
- Executive summary provides a multidimensional maturity view, top three gaps and recommended next steps
- Flexible delivery: Delivered either on-site or remotely

Specifications

Table 1. Cyber Resilience Advisory Workshop. Service features

| Feature | Delivery specifications |
|---|--|
| Cyber Resilience Advisory Workshop | <p>This workshop focuses on the implementation of the Cyber Resilience Advisory workshop by qualified HPE consultants.</p> <p>Engagement length is typically, a two-to-three-hour workshop and short report creation and sharing after the workshop conclusion.</p> <p>Under this service feature, HPE provides the following:</p> <ul style="list-style-type: none">– Mobilizes the HPE team– HPE will collaborate with the Customer to find a mutually agreeable workshop session date, time, video conference tool to be used, and if necessary physical meeting location– One (1) workshop session, not to exceed three (3) hours in length, with moderate and structured discussion on ransomware and malware– As part of this workshop, we will share information that will introduce Customer participants to the topic, sharing the methods and practical examples of cyber resilience scenarios and best practices to manage– HPE consultants will also ask and debate interesting and important aspects of cyber resilience, critical scenarios such as ransomware and strategies to protect <p>As a formal outcome of the workshop, HPE consultants will share a short high-level report mapping the workshop highlights. As part of the report, HPE will recommend the next high-level steps to define the transformation initiative to improve the overall Customer’s cyber-resilience posture.</p> |
| Deliverables | <p>Simplified high-level PowerPoint-based report showing summary highlights of the workshop discussions, recommendations and the next steps.</p> |

Cyber Resilience Readiness journey

Organizations need a cyber resilience readiness journey because threats and the operating environment have outpaced ad hoc defenses. Ransomware, data loss, and outages now target hybrid-cloud workloads and critical services that underpin SLAs. A readiness journey creates a structured plan to assess maturity, prioritize what matters, and strengthen people, processes, and technology so the organization can withstand, respond to, and recover from major incidents.

Regulatory frameworks such as NIS2 and DORA raise the bar: organizations—especially in critical and financial sectors—must demonstrate operational resilience with clear communications, incident reporting, and proven recovery capabilities. Meeting these standards requires a coordinated program with defined governance, cross functional awareness, tested procedures (for example tabletop exercises), and continuous improvement aligned to business priorities.

Practically, a readiness journey helps the enterprise:

- Convert business risks (ransomware, outages, limited data access) into prioritized resilience requirements for hybrid cloud.
- Validate and strengthen decision making, escalation, and recovery via exercises and measurable KPIs.
- Align SLAs, continuity plans, and regulatory obligations so critical services stay available and compliant.
- Build a sequenced roadmap of technology, configuration, and process improvements using best practices and specialist expertise.

Begin the Cyber Resilience Readiness journey with an end-to-end approach that assesses capabilities, validates response plans through realistic exercises, develops tailored incident playbooks, and establishes a sustained program to embed resilience. The four service modules have been designed as part of this journey:

- Cyber Resilience Readiness Assessment: review people, processes, technology, and governance to map maturity, prioritize services, identify gaps, and produce a remediation roadmap.
- Cyber Resilience Tabletop Exercise: scenario simulations to test decisions, communications, escalation, and recovery, yielding prioritized recommendations.
- Cyber Incident Response Plan Development: tailored, regulation aware incident plans and communication modes, playbooks for high impact scenarios, escalation workflows, and ties to business continuity and legal requirements.
- Cyber Resilience Program Plan and Development: set governance, roles, KPIs, service catalog, operational processes, and continuous improvement to institutionalize resilience and maintain readiness.

Cyber Resilience Readiness Assessment

Service overview

A targeted review of people, processes, technology, and governance to map maturity, prioritize critical services, identify vulnerabilities and gaps, and produce a practical roadmap of remediation and improvement actions.

During the execution of this service, HPE consultants will do a review of Cyber Resilience practices using HPE Cyber Resilience framework based on best practices: Asset Management, Controls Management, Configuration and Change management, Vulnerability Management, Incident Management, Service Continuity management, Risk Management, Supply Chain, Training and Awareness, Situational Awareness.

Service benefits

- Delivers visibility and assurance to stakeholders on the enterprise's cyber resiliency capabilities and mission alignment
- Evaluates organizational/service resilience against cyber threats that considers processes, technologies and organization (people) dimensions across corporate actors who participate in business resiliency
- Provides a risk prioritized road map to enhance capabilities, processes and security controls to reduce risk exposure

Service feature highlights

- Assesses an organization's readiness to detect, react and recover to a cyber event
- Evaluates cross-domain and enterprise processes and capabilities to identify, detect, respond and recover from a cyber incident based on maturity framework
- Two service options:
 - Organizational scope. Evaluates cyber resilience at an organizational level, with cross-service consideration based on the agreed Statement of Work (SoW)
 - Critical Service scope. Evaluates cyber resilience for the specific critical service, its IT infrastructure and dependencies included in the agreed SoW

Specifications

Table 2. Cyber Resilience Readiness Assessment. Service features

| Feature | Delivery specifications |
|---------------------------------|--|
| Kick-off and Preparation | <p>An HPE project manager will work with the Customer remotely to:</p> <ul style="list-style-type: none"> – Initiate the project with a kickoff meeting and organize remote follow-up and status meetings, including discussions of requirements – Identify and review the service prerequisites and highlight any actions required of the Customer to meet those prerequisites – Explain and distribute questionnaires – Schedule the on-site delivery of consultative services – Initial data gathering, process and procedures: <ul style="list-style-type: none"> • Information security management system • Incident response • Crisis management • Disaster recovery and backup • Business continuity |
| Discovery | <p>Running individual workshops for evaluating ten domains:</p> <ul style="list-style-type: none"> – Asset management – Controls management – Configuration and change management – Vulnerability management – Incident management – Service continuity management – Risk management – External dependency management – Training and awareness – Situational awareness |
| Gap analysis and roadmap | <ul style="list-style-type: none"> – Method validation and target Future state – Identify and analyze gaps – Prioritize and plan with cost Benefit analysis |
| Report and Presentation | <ul style="list-style-type: none"> – Report preparation – Maturity evaluation – Findings and recommendations – High level plan to improve cyber resilience – Final presentation of results – Activity closure and sign-off |
| Deliverables | <p>The HPE project team will work with the Customer to deliver:</p> <ul style="list-style-type: none"> – Report with assessment across ten domains – Prioritized list of actions for cyber resilience improvement |

Cyber Resilience Tabletop Exercise

Service overview

A scenario-driven tabletop exercise that validates decision-making, communications, escalation paths, and recovery procedures across the organization, producing concrete observations and prioritized, actionable recommendations to strengthen overall response capabilities. Designed around realistic ransomware scenarios, the exercise tests people, processes, and technologies in a safe, controlled environment to reveal gaps and opportunities for improvement before a real incident occurs.

HPE will design and facilitate the full tabletop engagement, walking stakeholders through each stage of a simulated ransomware attack—from initial detection and containment to recovery and post-incident lessons learned. The session includes role-based injects, facilitated discussion, and live evaluation of cross-organizational procedures, communications, and handoffs. Following the exercise, HPE delivers concise findings report with risk-ranked remediation actions, updated playbook recommendations, and suggested improvements to governance, escalation flows, and recovery plans to enhance readiness and reduce time-to-recovery.

Service benefits

- Provides a preview of how the organization would detect, react and respond to a cyber attack
- Lessens the likelihood and impacts from new and modern cyber threats such as ransomware attacks
- Evaluation of cyber resilience processes and procedures to ensure proper business recovery after a high-impact cyber threat

Service feature highlights

- Tabletop exercise with a simulated ransomware attack to test processes, procedures and people readiness
- Focus on crisis management, security incident management, business continuity, and disaster recovery processes

Specifications

Table 3. Tabletop Exercise. Service features

| Feature | Delivery specifications |
|---------------------------------|--|
| Kick-off and Preparation | An HPE project manager will work with the Customer remotely to: <ul style="list-style-type: none">– Initiate the project with a kickoff meeting and organize remote follow-up and status meetings, including discussions of requirements– Identify and review the service prerequisites and highlight any actions required of the Customer to meet those prerequisites– Business engagement session– Exercise definition– Tabletop workshop planning |
| Exercise Execution | <ul style="list-style-type: none">– Execution of the Tabletop Exercise<ul style="list-style-type: none">• Intro and setting scene• Describe scenario• Evaluate through a sequence of events• Debrief• Closing by business leader |
| Evaluation and Report | <ul style="list-style-type: none">– Report preparation with GAP analysis<ul style="list-style-type: none">• Maturity evaluation• Findings and recommendations• Action plan for improvement |
| Deliverables | The HPE project team will work with the Customer to deliver: <ul style="list-style-type: none">– Template with Tabletop exercise– Report with evaluation and notes from observers |

Cyber Incident Response Plan Development

Service overview

In today's evolving threat landscape, a generalized cyber incident response plan is insufficient to effectively manage complex cyber incidents. Regulatory frameworks such as NIS2 and DORA now require organizations to implement tailored incident response plans with defined communication protocols for critical cyber events. This advisory service supports enterprise CISO teams in developing customized incident response plans that specifically address critical cyber incidents, ensuring full compliance with relevant regulatory requirements.

Service benefits

- Builds standard capability in focused response to critical cyber incidents
- Reduce the vulnerability to large scale business disruption and/or supply chain disruption and/or geopolitical and/or industry specific threats
- Fulfill cyber response specific regulatory obligation
- Optionally train resources and test the response plan to guarantee its successful execution

Service feature highlights

- Provides an incident response plan that addresses programmatic and threat-based approach to critical cyber incidents based on applicable regulations
- Optionally provides a Test Plan and Training and Awareness Plan will ensure that execution of incident response plan is well rehearsed to ensure successful execution

Specifications

Table 4. Cyber Incident Response Plan Development. Service features

| Feature | Delivery specifications |
|---------------------------------|--|
| Kick-off and Preparation | An HPE project manager will work with the Customer remotely to: <ul style="list-style-type: none">– Initiate the project with a kickoff meeting and organize remote follow-up and status meetings, including discussions of requirements– Information gathering on applicable regulatory framework, compliance controls, and existing incident response processes |
| Plan development | <ul style="list-style-type: none">– Review of the existing Security Incident Response Process– Outage scenario development with response and recovery approaches for critical threat use cases– Incident Response Plan Development– Test Plan Development (add-on)– Training Plan Development (add-on) |
| Review and report | <ul style="list-style-type: none">– Joint review of Gap assessment report– Presentation of Incident Response Plan– Feedback incorporation into Incident Response Plan– Presentation and review of Test Plan (add-on)– Presentation and review of Training and Awareness Plan (add-on) |
| Deliverables | <ul style="list-style-type: none">– Incident response plan document– Test Plan (optional add-on)– Training and awareness (optional add-on) |

Cyber Resilience Program Plan and Development

Service overview

In today's threat landscape and regulatory environment, a generic response approach is no longer sufficient. Regulators and stakeholders expect a demonstrated ability to prevent, detect, respond to, and recover from critical cyber events, with specific plans, defined communication channels, and tested procedures that protect essential services and reduce economic impact. Organizations also face reputational risk and operational disruption if they cannot maintain continuity during incidents, making a structured cyber resilience program essential for sustained confidence and compliance.

This service provides a comprehensive framework to design, implement, and continuously improve an enterprise-wide cyber resilience program. It includes a program plan and governance setup, a cybersecurity resilience framework and service catalog, readiness for critical services, and targeted tabletop exercises, along with clear deliverables such as scope definitions, maturity dashboards, readiness roadmaps, and a management framework. Through structured risk assessment, gap analysis, incident response development, and testing, the service enables organizations to meet regulatory requirements while enhancing continuity, compliance, brand trust, and overall resilience.

Service benefits

- Minimize economic impact. Build confidence, prepare for cyberattacks and enable recovery from disasters more quickly, reducing financial losses from unplanned outages.
- Remain compliant. Enhance your ability to assess the security status of your organization. Identify loopholes that could lead to non-compliance and fill in the gaps to ensure legal and regulatory requirements are met.
- Improve brand reputation. Incidents can affect reputation and undermine Customer trust. Cyber resilience provides a solid foundation, assuring Customers of a reliable and dependable framework for their cybersecurity needs.
- Sustain business continuity. Mitigate risks and minimize the impact of cyber threats with a robust cyber resilience program.

Service feature highlights

- Provides a program plan that addresses programmatic and scope-based approach
- Defines a Cyber Resilience improvement plan to close gaps with proven expertise and a continuous improvement approach
- Defines a Cyber Resilience Process Framework and guidelines to protect the organization and the most critical services against high-impacted cyber threats

Specifications

Table 5. Cyber Resilience Program Plan and Development. Service features

| Feature | Delivery specifications |
|---|---|
| Governance | <ul style="list-style-type: none"> – Program plan: Define the overall objectives, scope, milestones, and resource commitments to guide cyber resilience initiatives. – Service management: Establish processes to coordinate, deliver, and monitor security-related services and support across the organization. – KPI and SLA management: Set clear, measurable performance indicators and service level agreements to drive accountability and continuous improvement. – Escalation management: Implement a structured path for timely escalation of incidents and issues to the appropriate roles for resolution. – Progress reporting: Provide regular, concise updates on status, risks, and outcomes to stakeholders to inform decision-making. |
| CR readiness | <ul style="list-style-type: none"> – Review of the existing Security Incident Response Process – Outage scenario development with response and recovery approaches for critical threat use cases – Incident Response Plan Development – Test Plan Development (add-on) – Training Plan Development (add-on) |
| Cyber Resilience Framework development | <ul style="list-style-type: none"> – Define CR Service catalogue – Develop processes – Roles and responsibilities – Create CR architecture guidelines – Program plan to operationalize CR practice |
| CR readiness for critical services | <ul style="list-style-type: none"> – Preparation – Discovery – Gap analysis and roadmap – Report and presentation |
| Tabletop Exercises | <ul style="list-style-type: none"> – Preparation – Perform the exercise – Evaluation and report |
| Deliverables | <ul style="list-style-type: none"> – Cyber resilience scope definition – Maturity Dashboard – CR Readiness report and roadmap – CR Management framework – CR program plan – CR readiness report for critical services – Tabletop exercises |

Disaster Recovery Modernization journey

Protecting your digital enterprise requires an optimum IT infrastructure with a cohesive continuity and disaster recovery (DR) strategy covering the entire triad of confidentiality, integrity, and availability. Disaster Recovery modernization is key to business continuity in the event of a disaster. Hewlett Packard Enterprise helps Customers meet this challenge by providing four distinct, but related offers. The essential components of Disaster Recovery Modernization journey are

- Business Impact Analysis
- Disaster Recovery Capability Maturity Analysis,
- Disaster Recovery Plan Refresh

Business Impact Analysis is the foundation of a DR strategy by identifying business critical services and defining their recovery objectives. Disaster Recovery Capability Maturity Analysis provides a comprehensive assessment to help ensure critical data availability during contingency scenarios whether on-premises or within the cloud. Although disasters may not always be avoidable, having an up-to-date DR plan helps reduce potential damage and expedite recovery operations where Disaster Recovery Plan Refresh module helps to ensure that your DR plans are current and optimized for your environment

HPE can assist Customers with their Disaster Recovery transformation that can include recovery strategy, design, deployment, DR plan refresh, and exercises with the modules described in the following sections:

- Business Impact Analysis
- Disaster Recovery Capability Maturity Analysis
- Disaster Recovery Plan Refresh

Business Impact Analysis

Service overview

Business Impact Analysis is designed to assist Customers evaluate their business process criticalities and the associated recovery requirements. This service is designed to help identify critical processes to help you assess the continuity of your business operations and the urgency of recovery and resumption in case of disaster. The service uses multiple ratings to help you evaluate the significance of various impacts on BC, based on the potential effects of the downtime of crucial processes on your business. For each in-scope process, the assessment helps to identify its recovery parameters, in terms of the minimum resources required, and helps you determine the maximum downtime and data backup parameters of a significant outage during peak and nonpeak business seasons, expressed as factors of time. The assessment can also help you identify vital resources and dependencies in terms of IT and infrastructure requirements, documentation, third parties, and related upstream or downstream processes. A business impact analysis (BIA) is a point-in-time exercise that is based on the information provided during the information gathering phase of the service and the associated timeline for collecting and evaluating this information as part of the delivery of this service.

This is a fixed-price fixed-scope service for delivery at a single site. A range of service delivery options are available, based on the number of processes (defined as a cluster of related activities that produce a defined outcome) to be analyzed.

Service benefits

- Provides a concise, strategic view of the resources and critical operations needed to meet business continuity objectives
- Helps categorize the in-scope business processes within the organization into various criticality buckets
- Determines allowable outages, essential data needs and minimum operating requirements for the process to limit the overall impacts
- Creates an evidence-based foundation for prioritizing and funding recovery, prevention, and mitigation initiatives.
- Provides insight into essential requirements that safeguard the organization's brand, enhances Customer satisfaction, and mitigate financial and legal impacts

Service feature highlights

- Utilizes a consulting approach to facilitate data gathering and review of relevant documentation
- Identify critical business processes along with their dependencies, resource requirements, and recovery priorities.
- Classification of in-scope processes by criticality using a standardized scoring model
- Define recovery parameters such as RTO (Recovery Time Objective), RPO (Recovery Point Objective), MOR (Minimum Operating Requirements)
- Provides recommendations to strengthen business continuity

Specifications

Table 6. Business Impact Analysis. Service features

| Feature | Delivery specifications |
|---------------------|--|
| Kickoff | <ul style="list-style-type: none">– Initiate the project with a kickoff meeting and organize remote follow-up and status meetings, including discussions of requirements– Identify and review the service prerequisites and highlight any actions required of the Customer to meet those prerequisites– Schedule the on-site delivery or off-site delivery of consultative services– Review of business objectives with key stakeholders– Outline service scope, process and methodologies |
| Discovery | <ul style="list-style-type: none">– Distribute questionnaires and provide a better understanding of the BIA process– Perform detailed process walkthroughs to understand and document business processes, including key activities, inputs, outputs, and controls– Conduct BIA workshops and/or questionnaires to collect information from business stakeholders– Identify and document all upstream and downstream dependencies, such as people, systems, third-party services etc. |
| Analysis | <ul style="list-style-type: none">– Perform an impact analysis of business processes to evaluate the consequences of disruptions– Identify critical business processes for continuity of business operations– Define recovery objectives (RTO and RPO) and recovery priorities for each critical business process or functions– Consolidate and document all business processes, criticality ratings, their dependencies, and recovery objectives and obtain review and sign-off |
| Deliverables | <ul style="list-style-type: none">– Baseline of business objectives– Impact severity matrix– List of critical processes with interdependencies– Defined RTO/RPO, and recovery priorities.– Recommendations to strengthen Business Continuity– Executive summary of BIA Report |

Service eligibility

Business Impact Analysis is a packaged consulting service available in a range of three SKU service-level options.

Consult an HPE sales representative for guidance on which of these packaged consulting service SKUs is most appropriate to the Customer's requirements. Requirements outside these parameters can be provided at an additional charge, based on a mutually agreed-upon SOW reflecting the Customer's specific requirements.

Disaster Recovery Capability Maturity Analysis

Service overview

Ever-changing hybrid environments need a formal assessment to understand the maturity of disaster recovery (DR) capabilities, prioritize improvements, and provide assurance to management and regulators that recovery objectives are achievable.

The DR Capability Maturity Assessment evaluates availability and recovery gaps across your hybrid IT infrastructure, including on-premises and cloud environments. Our comprehensive technical review identifies gaps, vulnerabilities, and maturity levels, and validates readiness against recovery objectives across primary and secondary data centers. We deliver a clear, prioritized roadmap to strengthen your disaster recovery posture, aligning your current state with short- and long-term resilience goals. Enable business continuity and minimize downtime with actionable insights tailored to your needs.

Service benefits

- Accelerate the evaluation between availability objectives against your actual IT environment recovery capabilities
- Independent, vendor-agnostic review and recovery analysis of people, processes, and technology
- Collaborate on a unified vision for your DR hybrid cloud infrastructure
- Help improve BC and availability of critical applications and services utilizing optimum protection, high availability, clustering, failover, and automation
- Help to improve cost efficiency and management and reduce risks

Service feature highlights

- Outline DR objectives and availability requirements
- Evaluate service-level agreements (SLAs) on critical services and applications
- Interactive analysis workshops
- One-on-one interviews with key stakeholders
- Accelerated technical data gathering and validation
- Construct a gap analysis of recovery inefficiencies and risks around processes, technology, personnel
- Analysis recommendation pros-and-cons exercises
- Outline a high-level road map of continuity and DR improvement recommendations
- Both on-site and off-site delivery efforts

Specifications

Table 7. Disaster Recovery Capability Maturity Analysis. Service features

| Feature | Delivery specifications |
|---------------------|--|
| Kickoff | <ul style="list-style-type: none">– Initiate the project with a kickoff meeting– Organize follow-up and status meetings, including discussions of requirements for the service– Identify and review all service prerequisites and any actions required by the Customer to meet them– Schedule the on-site or off-site delivery of consultative services– Review of business objectives with key stakeholders– Outline service scope, process and methodologies |
| Discovery | <ul style="list-style-type: none">– Verify the technical environment, requirements, and prerequisites– Perform facilitated workshops with key members of each business unit– Perform data discovery through interviews and questionnaires with the Customer’s key personnel– Deploy data collection scripts (where applicable)– Review DR plan, runbooks, recovery objectives, strategies, processes, methodologies and respective reports |
| Analysis | <ul style="list-style-type: none">– HPE Services consultants will gather all information collected and begin the analysis phase:– Create a gap analysis of issues found, negative business impact outlined, and remedial recommendations reviewed– Compare gaps against business objectives– Review findings and options with key technical personnel– Highlight recommendation options and benefits– Create a high-level road map for improvement based on priority, cost, risks, time frame, and benefits |
| Deliverables | <ul style="list-style-type: none">– Document objectives, findings, supporting data, recommendations, benefits, and high-level road map that will be presented to the key stakeholders– Provide executive summary to the key stakeholders |

Service eligibility

The Disaster Recovery Capability Maturity Analysis service is based on a custom scope depending on the needs and requirements of a customer. Consult an HPE sales representative for guidance on scoping of requirements, with the assistance of an HPE security architect, based on a mutually agreed-upon SOW reflecting the Customer’s specific requirements.

Disaster Recovery Plan Refresh

Service overview

DR (Disaster Recovery) is an organization's ability to respond to and recover from an event that negatively affects business operations. The goal of DR methods is to enable the organization to regain the use of critical systems and IT infrastructure as soon as possible after a disaster occurs. To prepare for this, organizations often perform an in-depth analysis of their workload environment and create a formal document to follow during a crisis, known as a DR plan.

Many businesses are required to create and follow a specific process for DR to meet regulatory compliance. Failure to have DR procedures in place and documented can result in legal or regulatory penalties, extend the amount of time it takes to restore operations, or not be able to meet SLA requirements, not to mention data/revenue loss!

Thinking about disasters before they happen and creating a plan for responding can provide many benefits. It raises awareness about potential disruptions and helps an organization prioritize its mission-critical functions. It also provides a forum for discussing these topics and making careful decisions about how to best respond in a low-pressure setting.

During this interactive service, HPE brings a new perspective and experience on availability and recovery, by helping to ensure proper procedures are in place to quickly respond to a disaster event, with recovery personnel and their responsibilities defined, and recovery processes for critical business functions documented for all known disaster scenarios.

An organization should consider its DR plan as a living document. Regular DR testing should be scheduled to ensure the plan is accurate and will work when recovery is required. The plan should also be evaluated against DR criteria whenever there are changes in the business or IT environment that could affect your DR response.

Service benefits

- Help ensure BC and DR of critical business functions utilizing a well-documented DR plan
- Improve recovery response during a disaster event utilizing outlined procedures
- Enhance recovery efforts during a disaster with vetted processes to meet recovery SLAs
- Help ensure DR regulatory and business compliance, along with proof of due diligence for insurance companies
- Help to reduce DR risks with a DR plan review to infuse needed updates, including but not limited to, additional outage scenarios / technology refresh / personnel changes, as well as new processes/procedures or tabletop exercises

Service feature highlights

- A DR policy statement, plan overview, and main goals of the plan
- Key personnel and DR team contact information and responsibilities
- Clear disaster-declaration runbook — rapid activation and immediate response
- Interactive analysis workshops on existing recovery strategies and capabilities
- One-on-one interviews with key stakeholders
- Analyze and document business-critical recovery processes using different data copies and recovery methods depending on the recovery scenario
- Both on-site and off-site delivery efforts

Specifications

Table 8. Disaster Recovery Plan Refresh. Service features

| Feature | Delivery specifications |
|-------------------------|---|
| Kickoff | <p>An HPE project manager will work remotely to:</p> <ul style="list-style-type: none"> – Initiate the project with a kickoff meeting – Organize follow-up and status meetings, including discussions of requirements for the service – Identify and review all service prerequisites and any actions required by the Customer to meet them – Schedule the on-site or off-site delivery of consultative services – Review of business objectives with key stakeholders – Outline service scope, process and methodologies |
| Discovery | <ul style="list-style-type: none"> – Verify the technical environment, requirements, and prerequisites – Perform facilitated workshops with key members of each business unit and critical business function – Perform data discovery through interviews and questionnaires with the Customer's key personnel – Inventory systems, applications, data stores, backups, and vendor dependencies. – Analyze all recovery processes and procedures for each critical business function – Deploy data collection scripts (where applicable) |
| Plan Development | <p>HPE Services consultants will gather all information collected and begin the documentation phase:</p> <ul style="list-style-type: none"> – Establish recovery priority tiers and sequencing based on SLA/RTO/RPO validation. – Draft disaster declaration criteria and decision matrix (severity levels, authorized declarants). – Draft DR policy statement, plan overview, and main goals of the plan – Key personnel and DR team contact information and responsibilities – Create Step-by-step instructions / runbook on how to declare a disaster event and disaster response actions – Document all business-critical functions with recovery objectives – Document recovery processes with different data copies and recovery methods depending on the recovery scenario |
| Deliverables | <ul style="list-style-type: none"> – Detailed DR plan (based on scope of service) – Facilitate review workshops (walkthroughs and tabletop exercise) to validate procedures and disaster declaration workflow |

It is highly advisable to undertake the [Business Impact Assessment](#) module if recovery objectives (SLAs) and priorities have not been clearly established.

Service eligibility

The Disaster Recovery Plan Refresh service is based on a custom scope depending on the needs and requirements of a customer. Consult an HPE sales representative for guidance on scoping of requirements, with the assistance of an HPE security architect, based on a mutually agreed-upon SOW reflecting the Customer's specific requirements.

Business Continuity Management Evolution journey

The Business Continuity Management (BCM) Evolution journey delivers a comprehensive set of services to build and mature a business continuity management framework. We assess current maturity, identify gaps, and develop a practical roadmap to improve capabilities and strengthen responses to disruptive events.

HPE Cybersecurity Services performs risk assessments for critical business processes and enhances existing BC plans to identify operational risks that could cause service disruption during incidents or crises. With continually changing environmental, technological, regulatory, and third-party conditions, risk management is now a strategic priority. Embedding proactive risk practices enables organizations to anticipate and manage emerging threats instead of merely reacting to them.

Risks and threats to businesses are on the rise

In today's connected world, losing access to critical operations can affect your business in many ways. Unplanned downtime and data loss can originate from many sources, including natural disasters, networks, power outages, hardware or software failures, human errors, or malicious acts. Additional risk comes from inflexible or inadequate infrastructure, data protection, and disaster recovery (DR) models. Best practices for BC must cover a wide range of scenarios.

In the evolving landscape of business continuity management (BCM), modernization is crucial as organizations face emerging risks that extend beyond traditional and legacy use cases. Cybersecurity threats, such as ransomware attacks, supply chain vulnerabilities, and data breaches, now pose significant disruptions that were not previously accounted for in conventional continuity planning. As regulatory compliance mandates increasingly require timely incident notification to authorities, businesses must reassess their strategies, BC plans, and crisis management procedures to ensure alignment with new requirements. Additionally, these evolving threats necessitate a thorough review of DR architectures and procedures to ensure resilience against cyber-induced disruptions. Organizations must adapt their recovery strategies to account for data integrity risks, cloud dependencies, and real-time response capabilities, integrating cybersecurity resilience into BCM frameworks to effectively address both operational and regulatory challenges.

HPE Services—Advisory and Professional Services can provide an expedited and fresh perspective of your Business Continuity Management program against business requirements to validate risk exposure.

Business continuity for the dynamic enterprise

In today's rapidly evolving business landscape, characterized by constant change, disruption, and heightened competition, the expectations for BC have significantly increased.

Organizations need to shift from reactive to proactive BC plans, being agile, adaptive, technology-driven, integrated, and holistic along with Customer-centric and continuously improving and scaling up and out. HPE Services can help identify gaps and provide a remediation road map to help ensure the optimum BC solution that is both fit for purpose and adaptive to business growth.

The key objectives of the HPE Cybersecurity Services offering include:

- Reviewing capabilities or environment to document current state infrastructure and strategy in relation to BC
- Identifying and evaluating potential threats or disruptions that could impact an organization's operations
- Developing mitigation strategies proactively to manage the risks and help ensure critical functions can continue during a disaster or disruption
- Helping businesses prioritize risks, enabling them to focus their BC planning efforts accordingly

Hewlett Packard Enterprise can assist Customers with their BCM needs with the following Services:

- Business continuity maturity assessment
- Risk assessment for business continuity
- Business continuity plan refresh (scenario development)

Business Continuity Maturity Assessment

Service overview

A Business Continuity Maturity Assessment evaluates an organization's current business continuity capabilities and effectiveness. It helps leaders make data-driven decisions to enhance organization resilience.

The service provides:

- Examine Organization's existing BC strategy, policies, processes and key metrics for its critical processes
- Determining the Maturity levels to measure progress against the industry's best practices
- Identify the continuity gaps and areas of improvement in their current BCM components
- Validates the overall effectiveness of the BCM program and its alignment with ISO 22301 standards
- Establishing a roadmap which outlines key recommendations/actions to advance through maturity levels

Service benefits

- Empower leaders to make data-driven decisions in shaping the organization's Business Continuity strategy.
- Enable organizations to optimize recovery strategies, resulting in faster response times and reduced operational downtime during a crisis.
- Ensures organization's business continuity strategies align with industry's best practices and regulatory standards, fostering compliance and excellence.
- Enhance overall resilience by realizing the current state, uncovering potential opportunities and areas of improvement to ensure the organization is fully equipped to manage any disruptive event.
- Strategic baselines enable organizations to continuously adapt and evolve in response to changing business conditions, emerging risks, and technological advancements.

Service feature highlights

- A wide-ranging analysis examines various business continuity components, with respect to services, policies, resources, dependencies, performance metrics.
- Various stakeholder engagements ensure the assessment is both applicable and functional.
- A scoring framework provides a clear measure of business continuity maturity levels.
- Realistic recommendations on BCM best practices to enhance organization's overall resilience.
- Evaluation of organization's continuity maturity against ISO 22301 supports effective certification preparation.

Specifications

During the implementation of the Business Continuity Maturity Assessment service, HPE consultants will do a review of the business and its environment as scoped and agreed upon.

Table 9. Business Continuity Maturity Assessment. Service features

| Feature | Delivery specifications |
|-------------------|---|
| Understand | <p>An HPE project manager will work with the Customer on-site and/or remotely as scoped in the SOW to:</p> <ul style="list-style-type: none"> – Initiate the project with a kickoff meeting and organize remote follow-up and status meetings, including discussions of requirements – Identify stakeholders and interviewers, relevant departments, and resources – Manage initial data gathering – BC/DR technical management organization chart, BCM program document, including scope, objectives, BIA, RA and BC/DR strategies in place (and detailed procedures, if applicable) – Identify existing Customer recovery pain points – Schedule the remote/on-site (if required) delivery of consultants/SMEs |
| Assess | <ul style="list-style-type: none"> – Run individual workshops to review the organization and its processes; including interviews with key Customer personnel if required to complement the workshops – Review The scope of the existing BCM documentation – Review of the BCM governance – Review BC personnel awareness, communications, and documentation – Review BCM operations and past exercises/invocations – Review BCM performance metrics monitoring, reporting, and improvement – Review questionnaires and initial responses, clarifications if any – Record observations and gaps, weaknesses etc. |
| Document | <ul style="list-style-type: none"> – Analyze results of all workshops, documents gathered, and questionnaires from a scope perspective – Analyze the BCM practices associated with key businesses process – Develop recommendation plans for gaps based on the priority – Document the assessment report |
| Report | <ul style="list-style-type: none"> – Detailed Business Continuity Maturity Assessment report – Executive Presentation |

Service eligibility

The Business Continuity Maturity Assessment service is based on a custom scope depending on the needs and requirements of a Customer. Consult an HPE sales representative for guidance on scoping of requirements, with the assistance of an HPE security architect, based on a mutually agreed-upon SOW reflecting the Customer's specific requirements.

Risk Assessment for Business Continuity

Service overview

Risk Assessment for Business Continuity pinpoints events that could disrupt operations, quantify their likelihood and impact, and recommend targeted treatments. Using ISO 22301, ISO 31000 and NIST SP 800-30/34, the engagement equips leaders with a clear, actionable roadmap to strengthen organizational resilience.

The service provides:

- Identify threats and vulnerabilities for critical services using ISO 22301 and NIST guidance
- Evaluate likelihood and impact; create heat maps and risk registers
- Measure control effectiveness and residual risk against defined appetite and best practices
- Prioritize risks; define mitigate, transfer, accept, avoid strategies with cost-benefit data
- Deliver executive report and roadmap supporting Business Continuity Plans

Service benefits

- Continuously assess your threat landscape helping ensure plans reflect current business environment
- Assess the likelihood, threats, impact, and risk ratings
- Create a nonstandard mitigation plan against risks to their business
- Identify dependencies between key business functions and risks
- Identify dependencies on third parties and associated risks

Service feature highlights

- Detailed walkthroughs to capture business-specific processes
- Facilitate sessions to identify risks and align stakeholders
- Define or Update risk assessment procedures and appetite
- Identify, analyze, and categorize risks by likelihood and impact
- Prioritize and develop plans based on risk appetite
- Deliver comprehensive reports on findings and mitigation progress

Specifications

Table 10. Risk Assessment for Business Continuity. Service features

| Feature | Delivery specifications |
|-------------------|---|
| Understand | <p>An HPE project manager will work with the Customer on-site and/or remotely as scoped in the Statement of Work (SOW) to:</p> <ul style="list-style-type: none"> – Kick-off workshop to confirm goals, scope, roles and responsibilities, timelines and communication cadence – Stakeholder and SME interviews/workshops to capture business processes, applications, sites, risk appetite and tolerance – Structured collection and review of existing BC and DR Policies, Diagrams, Incident logs and related documentation – Definition and agreement of Risk Assessment methodology, data collection templates and evaluation criteria – Issuance of an approved Project Plan and RACI matrix signed off by Customer and HPE |
| Assess | <p>The HPE project team will work with the Customer on-site and/or remotely as scoped in the SOW to:</p> <ul style="list-style-type: none"> – Facilitation of risk identification sessions using threat intel inputs, checklists and incident history – End-to-end mapping of threats, vulnerabilities and existing controls to every in-scope business process – Quantitative/Qualitative analysis of likelihood and impact to build a Risk Matrix and Heat Map – Creation of a comprehensive, prioritized Risk Register with clear ownership and residual risk ratings – Validation workshops with SMEs to confirm data accuracy and finalize risk scoring – Delivery of a Risk Heat Map and Prioritization Matrix highlighting “High” and “Moderate” exposures |
| Mitigate | <p>The HPE project team will work with the Customer to:</p> <ul style="list-style-type: none"> – Analysis of each significant risk (mitigate, transfer, avoid, accept) with cost/benefit considerations – Collaborative workshop to agree treatment priorities aligned with business objectives and compliance – Development of a time bound Risk Treatment Plan detailing actions, owners, resources and milestones – Definition of key risk indicators (KRIs), monitoring cadence and performance reporting framework – High level recommendations for enabling technologies, process changes and sourcing strategies |
| Document | <ul style="list-style-type: none"> – Comprehensive Risk Assessment Report – Detailed Risk Register, Heat maps, Treatment Plan – Executive Presentation |

Service eligibility

The Business Continuity Maturity Assessment service is based on a custom scope depending on the needs and requirements of a customer. Consult an HPE sales representative for guidance on scoping of requirements, with the assistance of an HPE security architect, based on a mutually agreed-upon SOW reflecting the Customer’s specific requirements.

Business Continuity Plan Refresh (Scenario Development)

Service overview

The service revitalizes your Resilience Program through a structured four phase methodology. Aligning with ISO 22301 and NIST 800-34, we assess current capabilities, identify gaps, and prioritize high impact disruption scenarios. The engagement culminates tailored BCP response playbooks that strengthen governance, recovery speed, and long-term continuity.

- Engagement refreshes Business Continuity Plan using ISO 22301 and NIST 800-34 frameworks
- Captures existing documentation, risks, stakeholders, and confirms scope, goals, governance
- Reviews BIA, threat assessments, and performs end-to-end continuity gap analysis
- Runs facilitated workshops to create pandemic, cyber, and supply-chain (examples) disruption scenarios
- Updates master BCP, policies, roles, and maintenance roadmap for long-term relevance
- Deliverables include refreshed BCP, scenario catalogue, prioritization matrix, RACI, executive summary deck
- Certified continuity professionals guide each step, ensuring best-practice alignment and quality outcomes

Service benefits

- Accelerate recovery readiness, reducing downtime costs and reputational damage during disruptive incidents
- Aligns resilience program with ISO 22301 standards and NIST guidance to satisfy auditors and regulators
- Identifies and prioritizes high-impact scenarios, supporting informed investment and risk decisions
- Clarifies roles, responsibilities, and communications, improving cross-functional response coordination
- Establish sustainable governance and review cadence to keep continuity plans current and effective

Service feature highlights

- Structured methodology: Understand, Assess, Scenario Development, Document – mirrors ISO 22301 lifecycle stages
- Scenario-specific response and recovery playbooks with decision trees, escalation paths, and actionable checklists
- Knowledge transfer and maintenance schedule empower internal teams, minimizing future consultancy dependence

Specifications

Table 11. Business Continuity Plan Refresh. Service features

| Feature | Delivery specifications |
|-----------------------------|--|
| Understand | <p>An HPE project manager will work with the Customer on-site and/or remotely as scoped in the SOW to:</p> <ul style="list-style-type: none"> – Conduct formal kick-off meeting to confirm scope, objectives, timeline, governance and communication cadence – Compile Stakeholder Register and RACI matrix; verify executive sponsor and single-point-of-contact (SPOC) – Collect and catalogue existing BCM and DR policies, BIA and RA reports, org charts, risk registers and related artefacts – Schedule and facilitate data gathering interviews/workshops with identified Business and IT SMEs – Establish secure information exchange mechanism and obtain required site/system access – Produce and obtain sign off on the detailed Project Plan with key milestones |
| Assess | <ul style="list-style-type: none"> – Execute structured BCP gap analysis against industry standards and regulatory expectations – Develop a Recommendations Matrix prioritizing remediation actions by risk, cost and compliance drivers – Host validation workshop to confirm findings, assumptions and data accuracy with SMEs and leadership – Deliver formal BCP Gap Analysis report highlighting strengths, weaknesses and improvement opportunities |
| Scenario development | <ul style="list-style-type: none"> – Define and agree scenario selection and prioritization criteria (impact, likelihood, regulatory) – Facilitate two or three cross functional workshops to generate and refine high risk scenarios (e.g., cyber-attack, pandemic, supply-chain disruption) – Map roles, responsibilities, decision authorities and communication flows for each selected scenario – Draft scenario-specific Response and Recovery playbooks including step-by-step actions, checklists and escalation paths – Conduct alignment session to validate and approve playbooks and ensure integration with existing incident processes |
| Document | <ul style="list-style-type: none"> – Refreshed Business Continuity Plan (BCP) – Scenario based Response and Recovery Playbooks – Executive Summary deck |

Service eligibility

The Business Continuity Plan Refresh service is based on a custom scope depending on the needs and requirements of a customer. Consult an HPE sales representative for guidance on scoping of requirements, with the assistance of an HPE security architect, based on a mutually agreed-upon SOW reflecting the Customer’s specific requirements.

Business Continuity Maturity Assessment

Service overview

A Business Continuity Maturity Assessment evaluates an organization's current business continuity capabilities and effectiveness. It helps leaders make data-driven decisions to enhance organization resilience.

The service provides:

- Examine Organization's existing BC strategy, policies, processes and key metrics for its critical products and services
- Determining the Maturity levels to measure progress against the industry's best practices
- Identify the continuity gaps and areas of improvement in their current BCM components
- Validates the overall effectiveness of the BCM program and its alignment with ISO 22301 standards
- Establishing a roadmap which outlines key recommendations/actions to advance through maturity levels

Service benefits

- Empower leaders to make data-driven decisions in shaping the organization's Business Continuity strategy.
- Enable organizations to optimize recovery strategies, resulting in faster response times and reduced operational downtime during a crisis.
- Ensures organization's business continuity strategies align with industry's best practices and regulatory standards, fostering compliance and excellence.
- Enhance overall resilience by realizing the current state, uncovering potential opportunities and areas of improvement to ensure the organization is fully equipped to manage any disruptive event.
- Strategic baselines enable organizations to continuously adapt and evolve in response to changing business conditions, emerging risks, and technological advancements.

Service feature highlights

- A wide-ranging analysis examines various business continuity components, with respect to services, policies, resources, dependencies, performance metrics.
- Various stakeholder engagements ensure the assessment is both applicable and functional.
- A scoring framework provides a clear measure of business continuity maturity levels.
- Realistic recommendations on BCM best practices to enhance organization's overall resilience.
- Evaluation of organization's continuity maturity against ISO 22301 supports effective certification preparation.

Specifications

During the implementation of the Business Continuity Maturity Assessment service, HPE consultants will do a review of the business and its environment as scoped and agreed upon.

Table 12. Business Continuity Maturity Assessment. Service features

| Feature | Delivery specifications |
|-------------------|---|
| Understand | <p>An HPE project manager will work with the Customer on-site and/or remotely as scoped in the SOW to:</p> <ul style="list-style-type: none">– Initiate the project with a kickoff meeting and organize remote follow-up and status meetings, including discussions of requirements– Identify stakeholders and interviewers, relevant departments, and resources– Manage initial data gathering BC/DR technical management organization chart, BCM program document, including scope, objectives, BIA, RA and BC/DR strategies in place (and detailed procedures, if applicable)– Identify existing Customer recovery pain points– Schedule the remote/on-site (if required) delivery of consultants/SMEs |
| Assess | <ul style="list-style-type: none">– Run individual workshops to review the organization and its processes; including interviews with key Customer personnel if required to complement the workshops– Review the scope of the existing BCM documentation– Review of the BCM governance– Review BC personnel awareness, communications, and documentation– Review BCM operations and past exercises/invocations– Review BCM performance metrics monitoring, reporting, and improvement– Review questionnaires and initial responses, clarifications if any– Record observations and gaps, weaknesses etc. |
| Document | <ul style="list-style-type: none">– Analyze results of all workshops, documents gathered, and questionnaires from a scope perspective– Analyze the BCM practices associated with key businesses process– Develop recommendation plans for gaps based on the priority– Document the assessment report |
| Report | <ul style="list-style-type: none">– Detailed assessment report– Socialization of the identified gaps/weaknesses– Assist with prioritization of addressing the identified gaps/weaknesses– Review/Presentation of findings |

Service eligibility

The Business Continuity Maturity Assessment service is based on a custom scope depending on the needs and requirements of a customer. Consult an HPE sales representative for guidance on scoping of requirements, with the assistance of an HPE security architect, based on a mutually agreed-upon SOW reflecting the Customer's specific requirements.

Risk Assessment for Business Continuity

Service overview

Our Risk Assessment for Business Continuity consulting service provides a robust framework for identifying, analyzing, and evaluating potential threats that could disrupt critical operations. By performing detailed process mapping and interactive workshops, we translate complex organizational nuances into a structured risk methodology that aligns with your specific risk appetite. We meticulously evaluate internal dependencies and third-party vulnerabilities to establish a clear hierarchy of risks based on their likelihood and impact. This comprehensive approach culminates in the development of bespoke mitigation strategies and detailed executive reporting, ensuring your leadership has the actionable insights needed to prioritize resilience and maintain operational stability in an evolving threat landscape.

Service benefits

- Continuously assess your threat landscape helping ensure plans reflect current business environment
- Assess the likelihood, threats, impact, and risk ratings
- Create a nonstandard mitigation plan against risks to their business
- Identify dependencies between key business functions and risks
- Identify dependencies on third parties and associated risks

Service feature highlights

- Process understanding and mapping—Performing detailed process walkthrough to understand business-specific process nuances
- Risk assessment workshop—Conducting workshop to help facilitate risk assessment and to provide a better understanding of business to stakeholders
- Defining of risk methodology and risk appetite—Define/Update procedure documents for risk assessment
- Identification, analyzability, and evaluation of risk—Perform risk assessment to identify potential risks, categorize risk based on its likelihood and impact
- Defining of risk mitigation plan—Based on organizations' risk appetite, help prioritize and build a risk mitigation plan
- Documentation and reporting—Provide detailed reports on findings, risk evaluation status, and risk mitigation goals

Specifications

Table 13. Risk Assessment for Business Continuity. Service features

| Feature | Delivery specifications |
|--|--|
| Understand—Kickoff | <p>An HPE project manager will work with the Customer on-site and/or remotely as scoped in the Statement of Work (SOW) to:</p> <ul style="list-style-type: none"> – Initiate the project with a kickoff meeting and organize remote follow-up and status meetings, including discussions of requirements – Identify stakeholders and interviewers, relevant departments, and resources – Manage initial data gathering - BC/DR technical management organization chart, BCM program document, including scope, objectives, BIA, BC plans, BC/DR strategies in place (and detailed procedures, if applicable), business processes utilizing the data center and DR data centers – Review existing recovery objectives (recovery time objective [RTO], recovery point objective [RPO], max allowable downtime, and more) – Review existing risk/threat analysis (including risk identification, risk assessment, and risk treatment), existing risk registers, and ERM policy and processes – Review the last BC/DR test results (if available) – Identify existing Customer recovery pain points – Achieve goals and objectives from the assessment – Schedule the remote/on-site (if required) delivery of consultants/SMEs |
| Assess—Workshops and interviews | <p>The HPE project team will work with the Customer on-site and/or remotely as scoped in the SOW</p> <ul style="list-style-type: none"> – Run individual workshops to review the organization and its processes; including interviews with key Customer personnel if required to complement the workshops – Review the scope of the existing BCM documentation – Review of the BCM governance – Review BC personnel awareness, communications, and documentation – Review BCM operation (with focus on risk and associated processes) – Review BCM performance metrics monitoring, reporting, and improvement – Review questionnaires and initial responses, clarifications if any |
| Mitigate—Analysis and recommendations | <p>The HPE project team will work with the Customer to:</p> <ul style="list-style-type: none"> – Analyze results of all workshops, documents gathered, and questionnaires from a BC/DR perspective – Analyze the risks associated with key businesses process – Develop mitigation plans for top/priority risks based on the recommendations – Develop recommendations for mitigations for all top/priority findings – Document the assessment report |
| Document | <ul style="list-style-type: none"> – Executive summary assessment report in Microsoft PowerPoint format – Detailed assessment report in Microsoft Word or Excel format – Review and validation of the risk register with the Customer risk owners and personnel involved in the assessment – Presentation of findings |

Service eligibility

The Risk Assessment for Business Continuity service is based on a custom scope depending on the needs and requirements of a Customer. Consult an HPE sales representative for guidance on scoping of requirements, with the assistance of an HPE security architect, based on a mutually agreed-upon SOW reflecting the Customer’s specific requirements.

Business Continuity Management Evolution Additional Service Capabilities

Additional service capabilities overview

HPE Services offer robust Business Continuity Management (BCM) capabilities that complement our broader service portfolio. We deliver tailored BCM services through flexible models, either project-based or as part of a continuous, as-a-service engagement. Our BCM Advisory Office can support clients in designing a fit-for-purpose framework, operationalizing activities, and managing ongoing operations such as risk assessments, BCM testing, and scenario planning. We also offer implementation and support services for BCM Automation platform to streamline key processes and workflows. Additionally, we can assist in establishing a comprehensive BCM management system, ultimately supporting and guiding through compliance and certification efforts with industry standards such as ISO 22301.

Business Continuity Management Automation overview

HPE services has capabilities and maintains partnership with software providers to Implements tool and technologies to automate business continuity processes, improving efficiency, accuracy, and speed of response during disruptions.

Business Continuity Management Automation solution benefits

HPE and Technology Alliance Partners collaborate to provide complete solutions to support the operationalization of BCM processes with the following functionalities:

- Unified Compliance and Resilience Platform - Combines HPE’s advisory and infrastructure strength with partner automation and governance engines.
- Accelerated Cloud Adoption - Enables faster, compliant cloud transformation through readiness assessments and ongoing controls.
- Continuous Compliance and Risk Management - From EUCS to NIS2, clients benefit from automated scoring, reporting, and evidence management.
- AI and Cybersecurity-Ready - Manage AI governance, DR/BC, and security regulations in one unified platform.

Business Continuity Management Advisory Office overview

HPE Services has capabilities to provide expert guidance and ongoing advisory support to develop, enhance, and sustain your business continuity management program aligned with evolving risks and business needs.

A BCM advisory office can be offered for our customers who want to modernize and/or develop full BCM capability and implement a management system. HPE can help you build and mature a dedicated BCM program office. As part of the scope and with a building block approach, we can combine described modules in Cyber Resilience portfolio or accommodate others to address specific needs the customer might have. This specific service implements and operationalizes BCM activities and processes and provides continuous support for compliance and certification processes.

Customer responsibilities

The Customer will:

- Allow HPE full access to all locations where the service is to be performed
- Assign a designated person from the Customer’s staff who, on behalf of the Customer, will grant all approvals, provide information, schedule meetings, provide meeting facilities, and otherwise be available to assist HPE in facilitating the delivery of this service
- Adhere to licensing terms and conditions regarding the use of any HPE service tools used to facilitate the delivery of this service, if applicable

- Provide a suitable work area for delivery of the service, including access to an outside telephone line, power, any network connections required, or remote access as applicable
- Provide all information necessary for HPE to deliver timely and professional remote or on-site delivery
- Be responsible for the security of the Customer’s proprietary and confidential information

Service limitations of all the service offerings

- Customer acknowledges and agrees that HPE may use resources outside the country of purchase for delivery of these services unless otherwise specified as part of a service feature description.
- HPE Consulting Services are technical in scope, designed to help improve HPE Cybersecurity Services capabilities. The services provided are subject to the limitations set forth in this data sheet and a mutually agreed-upon letter of agreement or SOW.
- HPE provides recommendations based on the accuracy and completeness of the information available at such time, along with the accuracy and completeness of any information provided by the Customer and obtained during this service.

General provisions / other exclusions

- HPE Cybersecurity Services – Cyber Resilience services are governed by the HPE standard terms for professional services.
- Services are provided during HPE standard local business hours and days excluding HPE holidays and as a single event over consecutive business days. Unless otherwise specified within an SOW.
- HPE reserves the right to charge, on a time-and-materials basis, for any additional work over and above the service package pricing that may result from work required to address service prerequisites or other requirements that are not met by the Customer.
- HPE reserves the right to reprice this service if the Customer does not schedule and provide subsequent delivery within 90 days of purchase.
- Any services provided outside of HPE standard business hours may be subject to additional charges.
- Portions of the service are delivered remotely or on-site, at HPE’s discretion.
- HPE’s ability to deliver this service is dependent upon the Customer’s full and timely cooperation with HPE, as well as the accuracy and completeness of any information and data the Customer provides to HPE.
- Deliverables are accepted upon presentation.
- Documentation created for this engagement will be available in PDF format unless otherwise specified.
- Availability of service features and service levels may vary according to local resources and may be restricted to eligible products and geographic locations.

Ordering information

To obtain further information and to order this service, contact a local Hewlett Packard Enterprise sales representative and reference the following service product number (s):

Table 14. Cyber Resilience Readiness journey. Ordering Information

| Service Module | SKU |
|---|---------|
| Cyber Resilience Readiness Assessment | Custom* |
| Cyber Resilience Tabletop Exercise | Custom* |
| Cyber Incident Response Plan Development | Custom* |
| Cyber Resilience Program Plan and Development | Custom* |

Table 15. Disaster Recovery Modernization journey. Ordering Information

| Service Module | SKU |
|--|--|
| Business Impact Analysis | Custom* or use the following SKUs for additional scope |
| 15 Processes / 1 Site / 15 days duration | H1XGOA1 |
| 30 Processes / 1 Site / 25 days duration | H36VXA1 |
| 60 Processes / 1 Site / 40 days duration | H36VYA1 |
| Disaster Recovery Capability Maturity Analysis | Custom* |
| Disaster Recovery Plan Refresh | Custom* |
| Cyber Resilience Program Plan and Development | Custom* |

Table 16. Business Continuity Management Evolution journey. Ordering Information

| Service Module | SKU |
|---|---------|
| Business Continuity Maturity Assessment | Custom* |
| Risk Assessment for Business Continuity | Custom* |
| Business Continuity Plan Refresh | Custom* |

* All services, including the Cyber Resilience Advisory Workshop service, can be ordered using HPE Security Consulting 5 Day Service SKU with a cover letter detailing the scope agreed with HPE and Customer.

- HPE Security Consulting 5 Days On-site Service - HU0U1A1
- HPE Security Consulting 5 Days Remote Service – H46QSA1

To obtain further information or order any of these services, contact a local HPE sales representative or HPE reseller and reference the HPE Cybersecurity Services – Cyber Resilience portfolio.

Learn more at

[HPE.com/services/support](https://hpe.com/services/support)

Visit HPE.com

[Chat now](#)

© Copyright 2026 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

This data sheet is governed by the Hewlett Packard Enterprise current standard sales terms, which include the supplemental data sheet, or, if applicable, the Customer's purchase agreement with Hewlett Packard Enterprise.

Excel, Microsoft, and PowerPoint are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All third-party marks are property of their respective owners.

a00158965ENW

HEWLETT PACKARD ENTERPRISE

hpe.com

