SUMMIT
TECH SOLUTIONS

Business Continuity Plan

Minimizing Disruption to Critical Functions

Presented by the ***Business Continuity Team:***

Jasmine Restrepo-Gaitan
Rafael Mejia Galvan
Vannellia Velez
Walter Bozzetti

Executive Vision

SummitTech Solutions is committed to ensuring the continuity of mission-critical IT and cloud services to its global clients, including Fortune 500 companies and government agencies.

In support of this commitment, this Business Continuity Plan (BCP) provides a structured approach to preparing for, responding to, and recovering from disruptive events.

Executive leadership, led by the Chief Information Security Officer (CISO), holds the authority to enforce this plan, allocate resources, and activate response teams.

The BCP reflects operational resilience, data protection, regulatory compliance, and transparent communication, with a focus on minimizing disruption and preserving client confidence.

Business Continuity Team

Name	Role on BCT	Responsibilities
Jasmine Restrepo-Gaitan	BCT Lead / Coordinator	Leads BCP development, coordinates team efforts, communicates with executive leadership, and ensures alignment with organizational goals
Rafael Mejia Galvan	Risk & Infrastructure Analyst	Assesses operational and IT risks, supports the BIA, and contributes to recovery strategies for critical infrastructure and IT systems
Vannellia Velez	Communications & Compliance Lead	Designs internal/external communication plans and aligns BCP with legal and compliance standards
Walter Bozzetti	Recovery & Testing Specialist	Develops recovery procedures for critical systems, contributes to DR plans, coordinates plan testing and simulation procedures

Key Contributors to BCP Development

Name / Title	BCP Contribution
Mike Tyson, Chief Information Security Officer (CISO)	Executive authority for BCP; oversees risk, cybersecurity, and regulatory alignment
Rita Ortiz, Director of Service Delivery	Ensures continuity of service delivery, incident response, and customer SLAs
Michael Tran, Director of Infrastructure Services	Advises on infrastructure resilience, recovery timeframes, and data center continuity
Bill Thompson, Director of IT Applications	Ensures BCP accounts for critical business applications like ERP, CRM, and SaaS
Tom Levy, Director of Finance and Accounting	Oversees financial continuity, payroll assurance, and compliance with financial regulations
Peter Jenkin, Director of Operations	Coordinates operational continuity and internal resource alignment during disruptions
Mateo Moss, Director of Legal Compliance	Ensures legal, contractual, and regulatory policies are integrated into the BCP

Policy Compliance Requirements

Business Continuity Policy

Defines organizational commitment to continuity, scope of the plan, recovery goals, and authority or responsibility structure.

Incident Response Policy

Describes how SummitTech identifies, reports, escalates, and responds to security and operational incidents.

Communication Policy

Provides guidance on internal and external communication during outages or major incidents.

Remote Work & Access Control Policy

Critical given 75% of staff work remotely, defines secure access, failover connectivity, and continuity responsibilities for remote teams.

Disaster Recovery Policy

Outlines procedures for recovering IT systems, infrastructure, and data after major disruptions.

Data Backup & Retention Policy

Specifies backup frequency, data retention durations, and storage locations for critical client and operational data.

Vendor Management Policy

Ensures third-party SaaS vendors are evaluated for risk and included in BCP considerations.

Regulatory & Industry Compliance Requirement

SOC 2 (Trust Services Criteria)

Availability, confidentiality, and processing integrity; requires documented recovery testing and incident handling procedures.

NIST 800-34 (Contingency Planning Guide)

For government clients; requires defined system recovery steps, impact analysis, and continuity strategies.

FedRAMP (for federal SaaS delivery)

Enforces stringent continuity, system security, and incident response documentation.

Information security and business continuity management; mandates BCP ownership, testing, and updates.

ISO 27001 / 22301

Contingency planning, data backup, disaster recovery, and emergency access procedures for ePHI.

HIPAA (for healthcare clients)

Requires data recovery and availability plans to ensure personal data is protected and accessible in outages.

GDPR / CCPA

Business Impact Analysis Recap

Maximum Tolerable Downtime (MTD)
Return Time Objective (RTO)
Recovery Point Objective (RPO)

Business Function/Process Recovery Metrics

Function	Process	Potential Disruptors	Impact Description	MTD	RTO	RPO
Infrastructure Services	**Remote Access Management**	• Appliance Failure • Natural Disasters • Misconfiguration • Cyber Attack (DDoS)	Disruption in VPN access would prevent remote employees (75% of workforce) from connecting to internal systems.	**24h**	**12h**	**15-30m**
Service Delivery	**Remote Monitoring & Management**	• Platform outage • Licensing Failure • Cyber Attack (Malware) • Insider Threat (Espionage)	Outage would leave the organization blind to system health and unable to respond to incidents	**24h**	**12h**	**15-30m**
Service Delivery	**Backup & Recovery**	• Appliance Failure • Cyber Attack (Ransomware) • Natural Disasters • Insider Threat	Loss of backup and recovery services would prevent data restoration after an incident, increasing the risk of permanent data loss and prolonged downtime	**12h**	**6h**	**15m**
Finance & Accounting	**Payroll**	• Platform outage • Insider Threat (Data Theft) • Database corruption • API Failure	If payroll systems are down, employee pay is delayed, leading to legal risk and loss of trust	**48h**	**36h**	**1h**
Operations	**Sales & Customer Relations**	• Platform outage • Insider Threat (Excess Privilege Misuse) • API Failure	CRM outage impacts sales, customer service, and relationship management, resulting in revenue loss and churn	**24h**	**12h**	**1h**
Legal Compliance	**Contractual Obligations Compliance**	• Platform outage • Insider Threat (Data Theft) • Cloud Storage Outage	Delayed access to legal documentation and audit records can result in non-compliance with regulations	**48h**	**36h**	**24h**

Risk Assessment & Threat Analysis

Threat Event: Cyber Attack (DDoS, Ransomware, Malware)

Asset Name	Asset Location	Vulnerability	Impact	Probability	Severity	Risk Factor	Mitigation
Veeam	On-premise	Backup repository encryption or deletion	Loss of backup data critical to restoration	4	5	**20**	Offline/offsite backup rotation, MFA, patching, immutability
ConnectWise RMM	Cloud	Remote access exploitation	Full network compromise through managed endpoint	4	5	**20**	Zero trust architecture, MFA, constant log monitoring
Cisco Firepower/ AnyConnect Secure Mobility Client	On-premise	VPN gateway exploitation	Network entry point exploited or denied	3	4	**12**	Regular firmware updates, VPN hardening, traffic inspection
SAP S/4HANA ERP	Cloud	Unpatched modules or misconfiguration	Payroll and thus business ops paralysis, financial loss	3	5	**15**	Role-based access, system patching, regular vulnerability scans
Salesforce	Cloud	API abuse, session hijack	CRM data breach, sales disruption	2	4	**8**	IP whitelisting, API rate limiting, SSO + MFA
Salesforce to DocuSign CLM Integration	Cloud	Token hijacking, unsecure integrations	Contractual obligations affected, legal & compliance risk	2	4	**8**	Secure API management, audit logging, encryption in transit

Risk Assessment & Threat Analysis (continued)

Threat Event: Insider Threat

Asset Name	Asset Location	Vulnerability	Impact	Probability	Severity	Risk Factor	Mitigation
Veeam	On-premise	Unrestricted access to backup storage by admins	Deletion or theft of critical backup data. Tampering with backup configurations and job schedules	3	4	**12**	Limit access based on role, implement immutable backups, monitor activity
ConnectWise RMM	Cloud	Misuse of admin privileges on managed devices	Tampering with scripts or client configurations	3	5	**15**	Review admin roles regularly, enforce change logging
Cisco Firepower/AnyConnect Secure Mobility Client	On-premise	Improper access control to network tools	Internal sabotage of firewall/VPN configuration	2	4	**8**	Limit admin access, use role separation, monitor commands
SAP S/4HANA ERP	Cloud	Access to confidential business workflows	Leakage of sensitive business and financial data	3	5	**15**	Restrict data views, log access to sensitive records
Salesforce	Cloud	Overly permissive sharing settings and lack of monitoring	Customer data loss or unauthorized data exports	3	4	**12**	Enable activity monitoring, alert on unusual downloads
Salesforce to DocuSign CLM Integration	Cloud	Weak user access controls and shared credentials	Exposure of confidential contracts or e-signature data	3	5	**15**	Enforce access governance, log integration actions, audit regularly

Risk Assessment & Threat Analysis (continued)

Threat Event: Natural Disaster (Flood, Winter Storms, Earthquakes, Severe Storms, Tornadoes, Wildfires)

Asset Name	Asset Location	Vulnerability	Impact	Probability	Severity	Risk Factor	Mitigation
Veeam	On-premise	Physical server damage or power loss	Inability to recover data during disaster	3	5	**15**	Geographic redundancy, offsite backups, UPS systems
ConnectWise RMM	Cloud	Cloud provider regional data center exposure	Service degradation or downtime affecting multiple clients	2	4	**8**	Use of multi-region deployment, cloud DR planning
Cisco Firepower/ AnyConnect Secure Mobility Client	On-premise	Failure of on-premise network access infrastructure	No remote access or firewall failure during disaster	3	5	**15**	Disaster recovery plans, redundant networking paths
SAP S/4HANA ERP	Cloud	Service disruption due to regional data center outages	Interruptions in core business operations and financial reporting	2	5	**10**	Contract with provider for geo-redundancy, cloud failover strategy
Salesforce	Cloud	Loss of access due to cloud region outage	Inaccessible CRM data impacting sales and customer support	2	4	**8**	Multi-region CRM deployment, offline data sync capability
Salesforce to DocuSign CLM Integration	Cloud	Interruption of API-based processes due to service unavailability	Delays in executing or validating signed agreements	2	4	**8**	Retry mechanisms in API calls, backup integration systems

Mitigation Strategies

IT & Data Recovery Mitigation Strategies

Strategy	Description
Geographic Redundancy	Real-time data replication between Seattle and Denver enables fast failover during disruptions.
Backup & Recovery	Offsite/cloud backups with defined RTO (2 hrs) and RPO (1 hr); restoration tested regularly.
Systems Hardening	Seismically braced infrastructure, UPS/generator redundance.
Predefined Disaster Recovery Plan	Predefined DR strategies with clustering, offsite syncs, and clear team roles for recovery.
Regular Disaster Recovery Drills	Annual failover drills validate readiness and refine recovery procedures.
Ready to Work Remote infrastructure	Business Microsoft 365 for deployment, make sure all employees laptop are up to date and ready to resume work at any time.

Workforce Continuity Mitigation Strategies

Strategy	Description
Emergency Communication Plan	Multi-channel alerts with up-to-date contact lists; redundant systems ensure message delivery.
Cybersecurity for Remote Work	Secure remote access via VPN + MFA; enforced endpoint protection and user awareness training.
Personal Preparedness	Employees maintain emergency kits and safe home office setups to remain resilient.
Alternate Work Arrangements	Pre-identified locations (e.g., coworking, client sites, coffee shops) for use if remote work is disrupted.
Disaster-Safe Work Location	Equip building 123 Main Street, Olympia, WA with support for essential staff, including power, connectivity, and emergency resources.
Remote Work Infrastructure	Laptops, EcoFlow Portable Power Station , and AT&T dedicated satellite internet access provided to all staff allowing remote work in case of emergency for up to a week.

Emergency Response and Crisis Management Plan

Involved Personnel and Their Role

Staff Name	Role Description	DDoS	Insider Threat	Earthquake
Michael Tran	Director of Infrastructure Services *Activates BCP and coordinates recovery operations*	✓	✓	✓
Leon Kim	Network Engineer *Mitigates the DDoS attack at firewall and network level*	✓	✓	✓
Steven Johnson	Cloud Computing Manager *Switches to backup VPN servers and cloud-based access*	✓		✓
Liam Brooks	System Administrator *Verifies user access and restores Role-Based Access Control (RBAC) settings*	✓	✓	✓
Maya Chen	Backup & DR Service Manager *Ensures availability and reliability of systems backups. Executes backup recovery.*		✓	✓
Nelson Mandel	Cybersecurity Engineer *Conducts real-time threat analysis and coordinates with external cybersecurity vendors*	✓	✓	

Triggers to Activate the BCP

DDoS

Extended VPN Downtime
- Remote access is disrupted for more than 15 consecutive minutes

Unusual Traffic Spikes
- Excessive inbound traffic is detected by monitoring tools, consistent with DDoS patterns (e.g., abnormal packet volume, connection floods)

Firewall & Security Alerts
- Detection of a DDoS attempt through firewall logs or IDS

Multiple Access Failures Reported
- Widespread user reports of being unable to connect remotely to company systems

Confirmation from ISP or Cloud Provider
- Internet Service Provider or cloud vendor confirm a DDoS attack targeting company infrastructure

Insider Threat To Backups (logic bomb)

Unusual Script Execution or Backup Job Modification
- Unexpected changes to Veeam backup job scripts, schedules, retention policies, or repository files.

Sudden Deletion or Encryption of Backup Files
- Backup data or metadata is being encrypted, corrupted, or deleted without a valid operational task.

Anomalous User Activity or Privilege Escalation
- A terminated employee account is reactivated, or a non-admin user attempts to modify backup configurations.

Anti-Tampering or Honeytoken Alert
- A decoy backup job (e.g., a honeytoken) is accessed or altered, designed solely to detect insider threats.

Earthquake

USGS ShakeAlert® Earthquake Early Warning System (EEW)
- Provides a notification of potential earthquake shaking via text alerts.

Warning Alarms Wailing for Earthquakes
- Provide alerts *seconds to minutes* before the damaging ground shaking from an earthquake arrives

Small tremors or foreshocks and ground uplift or subsidence
- Indicating that a high magnitude earthquake may follow.

DDoS Incident Response Plan

Phase	Timeframe	Actions
Before the Attack	Ongoing	• Test DDoS detection and mitigation systems, set abnormal traffic alerts. • Maintain backup configurations for network services. • Audit Role-Based Access Control (RBAC) and client access.
During the Attack	0 – 30 minutes	• Alert incident response team. • Block or filter malicious IPs using firewall rules. • Notify ISP or DDoS mitigation provider.
	30 – 60 minutes	• Switch network traffic to cloud-based failover infrastructure. • Implement rate limiting and geofencing (if applicable). • Communicate limited access mode to users.
	60 – 120 minutes	• Monitor traffic patterns continuously. • Begin compiling incident logs and access reports. • Isolate impacted systems if needed to protect internal networks.
Immediately After the Attack	2 – 3 hours	• Restore full network functionality (main + backup access) • Verify MFA and RBAC settings were not compromised. • Confirm endpoint client access is stable.
	3 – 4 hours	• Conduct post-incident review (PIR). • Document actions taken, root cause, and timeline. • Notify leadership and stakeholders. • Apply permanent firewall rules or service changes.
	4+ hours	• Update BCP and disaster recovery plans based on lessons learned. • Schedule user communication and security awareness follow-up.

Insider Threat Incident Response Plan

Phase	Actions
Before the Attack	**Background checks for IT Staff** • Verifying identity, employment history, education, and criminal records, among other details to minimize risk of onboarding potentially disgruntle or harmful employees. **Employee Offboarding Interviews & Immediate Privileged Access Revocation** • Exits interviews and immediately revoking all access credentials could help stops insider from acting post-exit **Audit Logging and Monitoring** • Audit privileged user sessions during the final weeks of employment **Backup Security Hardening** • Configure immutable backups (cannot be altered, deleted, or overwritten until retention period expires)
During the Attack	• Immediately isolate Veeam backup servers from the network. • Revoke any reactivated or dormant user accounts. • Identify and remove any planted scripts, scheduled tasks, or registry entries. • Perform forensic analysis to determine entry point, timeline, and scope. • Collect logs for legal and HR follow-up if insider threat is confirmed.
Immediately After the Attack	• Backup policies rebuild/configurations with version validation. • Conduct full DR simulation to test restore integrity. • Document all findings. • Update termination protocols and audit coverage for privileged users.

Earthquake Incident Response Plan

Phase	Actions
Before the Event	• Proactive training and safeguards. • Secure heavy equipment and servers with bolted racks and secured furniture. • Conduct regular earthquake drills ("Drop, Cover, Hold On"). • Clearly communicate evacuation routes and gathering points. • Back up key records and configurations offsite.
During the Earthquake	• Prioritize employee safety: follow "Drop, Cover, Hold On" protocol immediately. • In case it affects remote employees, have them seek safety away from windows and heavy objects. • Emergency notification system broadcasts alerts. • Automatic power shutdown may occur to prevent fire hazards.
Immediately After Shaking Stops	• Calm evacuation to designated open-air assembly areas away from buildings/power lines. • Floor wardens conduct roll call for employees and visitors. • First-aid teams address injuries. • Incident Response Team assesses building and data center damage. • Begin data center failover to Denver if Seattle data center is impacted.

Disaster Recovery Plan

Service Name: Remote Access / VPN Service

System Components Covered

- ❑ **VPN Servers** (Primary and Cloud-Hosted Backup)
- ❑ **Firewall & Network Security Systems** (Cisco Firepower)
- ❑ **MFA Systems** (e.g., Duo, Google Authenticator)
- ❑ **RBAC & Directory Services** (Active Directory/Azure AD)
- ❑ **Endpoint Access Clients** (AnyConnect, custom VPN clients)

Recovery Objectives

RTO (Recovery Time Objective): 2 hours – Resume remote access via backup infrastructure
RPO (Recovery Point Objective): 1 hour – All access policies, roles, and MFA settings restored
MTD (Maximum Tolerable Downtime): 4 hours

Disaster Recovery Plan

✅ Step 1: Assess and Confirm Outage

- ❑ Use monitoring tools (SIEM, NOC dashboards, firewall logs) to validate that **no users** can access via VPN.
- ❑ Confirm whether the issue is a **system failure**, **network configuration issue**, or **external attack (e.g., DDoS)**.
- ❑ Escalate to Michael Tran (**Director of Infrastructure**) to trigger the BCP/DRP.

🔁 Step 2: Activate Backup VPN Infrastructure

- ❑ **Switch to cloud-based VPN solution** (AWS, Azure, etc.) already configured with mirrored access rules.
- ❑ Update **DNS settings** or send out backup VPN client instructions.
- ❑ Notify users via alternate channels (email, Slack, SMS) with:
  - New connection instructions
  - Temporary access limitations (if applicable)
  - Security advisories

🔑 Step 3: Restore Authentication & Access Controls

- ❑ Reconnect **MFA system** (backup token or SMS-based verification).
- ❑ Sync RBAC permissions from **last good configuration backup** (within RPO limit of 1 hour).
- ❑ Enable access for **critical personnel first**, then full team once authentication systems are confirmed stable.

📊 Step 4: Monitor and Stabilize

- ❑ Actively monitor:
  - VPN load on backup system
  - Login activity (success/failure rates)
  - System logs for service errors or anomalies

Disaster Recovery Plan

📁 Step 5: Document Incident and Begin Root Cause Analysis

- ❑ Start compiling a full **incident log**: timestamps, teams involved, systems impacted.
- ❑ Begin forensic investigation:
  - Why did the primary VPN fail?
  - Were backup systems activated quickly enough?
- ❑ Assign Nelson Mandel (**Cybersecurity Engineer**) to review traffic patterns and provide incident report.

🔄 Step 6: Plan Reversion or Reinforcement

- ❑ Once primary VPN is restored:
  - Test for stability and security.
  - Gradually shift users back or keep cloud-based VPN as new primary (depending on findings).
- ❑ Update firewall and endpoint configurations accordingly.

📝 Step 7: Conduct Post-Incident Review

- ❑ Hold internal debriefing within 24–48 hours.
- ❑ Update DRP and BCP documents with lessons learned.
- ❑ Prepare an executive summary for leadership including:
  - Timeline of events
  - Actions taken
  - Downtime duration vs. RTO/RPO goals
  - Recommendations

Key Controls

Control Area	Requirement
Physical Security	Equip server rooms with vibration-dampening racks and seismic anchoring.
Logical Access	Defining user roles and responsibilities, managing access privileges, and establishing procedures for granting and revoking access. Ensure that only authorized users can access specific systems and applications.
Fire Suppression	Install earthquake-safe, gas-based fire suppression systems (e.g., FM-200).
Data Redundancy & Load Balancing	Maintain mirrored systems across Seattle and Denver data centers. Content Delivery Networks (CDNs - Cloudflare, AWS Shield, Akamai) Load balancers to route traffic during spikes
Backup Integrity	Configure immutable backups, store encrypted, offsite/cloud backups; verify RPO/RTO compliance.
System Availability	Continuous Remote health checks on all servers utilizing SolarWinds
Testing & Validation	Conduct periodic failover drills to validate backup and recovery capabilities.
Incident Detection	SIEM integration with alert thresholds, Real-time monitoring and logging of traffic anomalies

BCP Communication Plan

Communication Channels

Internal	Employees, Executives, IT & Security Teams, HR	Email, Teams/Slack, SMS alerts
External	Clients/Customers, Vendors/Partners, Regulators, Media, Law Enforcement	Website, Social Media, Press Releases, Reports, Direct Email

Communication Triggers

- Extended system outage
- Safety or security is compromised
- Facility disruption or evacuation
- Major service impact

Approval Workflow

Role	Task
Mateo Moss, Director of Legal Compliance	Approves content for regulatory/legal compliance
Rita Ortiz, Director of Service Delivery	Leads external messaging and client coordination
Mike Tyson, CISO	Final approval for high-visibility communications

BCP Communication Plan

Communication Steps by Incident Phase

✅ **Before the Event**

- ❑ Maintain updated contact lists
- ❑ Draft templates for key threat scenarios
- ❑ Train communication team
- ❑ Conduct tabletop exercises

⛔ **During the Event**

- ❑ Notify leadership team and affected department heads
- ❑ Send employee alert (status & instructions)
- ❑ Notify clients (brief service update)
- ❑ Schedule executive updates every 30 mins
- ❑ Alert vendors (if needed)

⏳ **After the Event**

- ❑ Send system recovery notice
- ❑ File reports to regulators (if needed)
- ❑ Share summary with clients and executives
- ❑ Hold internal debrief

BCP Testing and Training

Training & Testing	Purpose & Benefits	Frequency	Personnel
Employee Training Program	• Builds "muscle memory" for crisis response. • Practical, action-oriented steps • Orientation for new hires, annual refreshers for all staff.	• Ongoing/New hires • Annually	• All Employees
Tabletop Exercises	• Structured team walk-through of disaster scenarios • Realistic scenarios with evolving details. • Identifies gaps or confusion safely before real events.	• Semiannually	• Team Leads • Executives
Full-Scale Simulations	• Intensive, realistic drills including technical failover tests. • End-to-end verification of BCP effectiveness. • Identifies issues overlooked by simpler tests.	• Annually (or key systems)	• Critical personnel • BCP Roles
Cross-Training and Succession	• Prepares alternate personnel for key BCP roles to avoid single points of failure. • Role rotation in exercises to ensure depth and capability.	• Continuous during training & exercises	• Semi-critical personnel
Continuous Testing Schedule	• Regular drills (quarterly communication, semiannual tabletop, annual full-scale). • Debrief after each test ensures continuous improvement. • Keeps BCP current and effective.	• Quarterly, Semiannual, Annual	• BCP Roles • Team Leads • Critical personnel

BCP Improvement and Maintenance

Living Document

- BCP regularly updated (at least annually & after significant events).
- Prompt reflection of new services, processes, locations, and partners.
- Clear version control with management approval.

Continuous Improvement

- Every test or real event informs plan updates:
  - Adjust procedures, checklists, training based on findings.
- Annual senior management reviews:
  - Address deficiencies; allocate resources for improvements.
- Promote a culture of proactive learning and refinement.

Post-Incident Reviews

- Conduct **After-Action Reviews** after incidents or exercises.
  - Evaluate success of recovery
- Regular audits and self-assessments:
  - Verify contact info, backup systems, compliance.
- Track key metrics:
  - Downtime duration, recovery rates, drill participation.

Ongoing Governance

- BCP maintenance led by **Business Continuity Team (BCT)**.
  - Regular updates on contacts, technical recovery steps, vendor assumptions.
- Stay current on emerging threats and best practices.
- Ensure constant readiness for effective crisis response.

Industry Best Practices

- Follow **ISO 22301's PDCA Model**:
  - **Plan**: Set BCP strategies
  - **Do**: Implement strategies
  - **Check**: effectiveness
  - **Act**: Continuously refine
- Leverage **NIST SP 800-34** guidelines for comprehensive contingency planning.

Application of AI in This Project

Throughout our Business Continuity Plan (BCP) for SummitTech Solutions, we used AI tools (e.g., ChatGPT from OpenAI) to help guide our research, structure content, and provide relevant examples.

OpenAI – ChatGPT (Prompt Engineering & Document Generation)
🔗 https://platform.openai.com/docs/guides/prompt-engineering
➞ Used for generating structured plans, DRP content, and response scenarios.

🤖 Prompts Used

Use Case	Prompt Example
DRP Template	“Can you help me write a Disaster Recovery Plan for Remote Access/VPN?”
Role Clarity	“What roles are responsible for developing BCP policies?”
Communication Plan	“What does a communication plan in a BCP look like with examples?”
Risk Scenarios	“List 3 different business-impacting disaster scenarios with actions before, during, and after.”

AI References & Sources

🔐 Frameworks & Standards

- **NIST SP 800-34 Rev. 1** – *Contingency Planning Guide*
  csrc.nist.gov/SP800-34
  ➤ Defines BCP phases: BIA, recovery strategies, testing
- **ISO 22301:2019** – *Business Continuity Management Systems*
  iso.org/22301
  ➤ Global BCP lifecycle standard with risk-based planning
- **FEMA Continuity Guidance Circular**
  fema.gov/CGC
  ➤ Continuity of operations for government & enterprise
- **CIS Controls v8** – *Availability & Resilience Controls*
  cisecurity.org/controls
  ➤ Security-focused controls for maintaining operations

🧰 Toolkits & Guides

- **Ready.gov – BCP Toolkit**
  ready.gov/business-continuity-plan
  ➤ Step-by-step BIA, risk analysis, continuity planning
- **SBA Emergency Preparedness Guide**
  sba.gov/prepare-emergencies
  ➤ Tailored for SMB disaster response and recovery
- **Harvard IT BCP Guide**
  huit.harvard.edu/BCP-Guide
  ➤ Templates for identifying critical functions & testing