



SUMMIT
TECH SOLUTIONS

Business Impact Analysis

Risk Assessment and Threat Analysis

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

Jasmine Restrepo-Gaitan

Rafael Mejia Galvan

Vannellia Velez

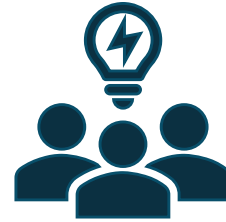
Walter Bozzetti

Business Objectives



Reliable IT Services

Proactive, scalable, and reliable solutions



Enterprise Solutions

Streamline operations and enable strategic goals



Downtime Mitigation

Reduce technological disruptions and outages



Cybersecurity & Compliance

Secure digital environments and mitigate risk

Company Overview

Company Snapshot

- Industry: IT & Cloud Services
- Headquarters: Seattle, WA
- Employees: 2,500
- Annual Revenue: \$750M
- Clients: Fortune 500 companies & government agencies

Technology & Operations

- Data Centers: Seattle, WA & Denver, CO
- Remote Workforce: 75%
- Critical Applications: ERP, CRM, cloud-based collaboration tools
- Service Focus: Managed IT, Cybersecurity consulting, SaaS delivery

Core Services



Cloud computing & data storage solutions

End-to-end provisioning, management, and monitoring of client Virtual Machines and associated storage ensuring high availability



IT infrastructure management

Ensures secure, stable, and high-performing IT environments that support both internal teams and client-facing services



Cybersecurity consulting

Strategic advisory on security protection including risk assessment, monitoring, threat detection and prevention, and incident response



SaaS-based enterprise software delivery

Delivery of a portfolio of trusted third-party SaaS-based enterprise software for ERP, CRM, and HR as a Managed Service Provider (MSP) and IT integrator.

Business Impact Analysis (BIA)

Purpose:

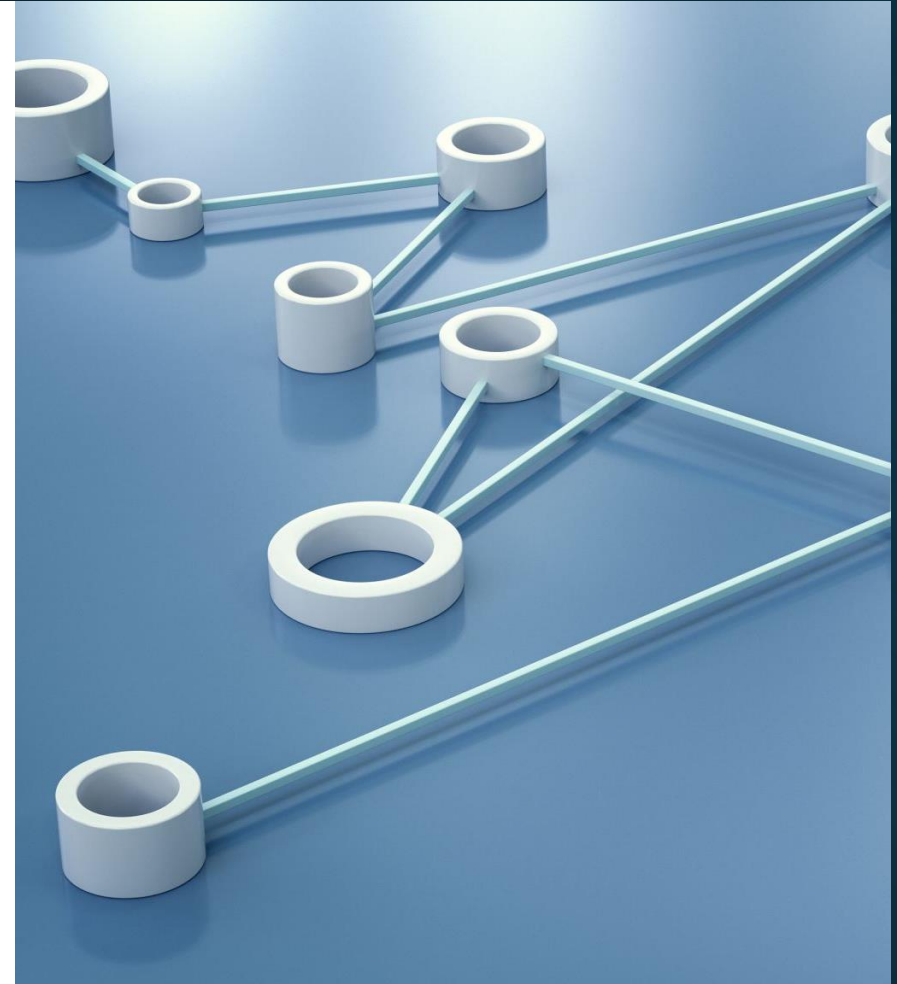
- Assess critical functions, processes, information systems, personnel, and suppliers crucial for business operations

Assessment Framework:

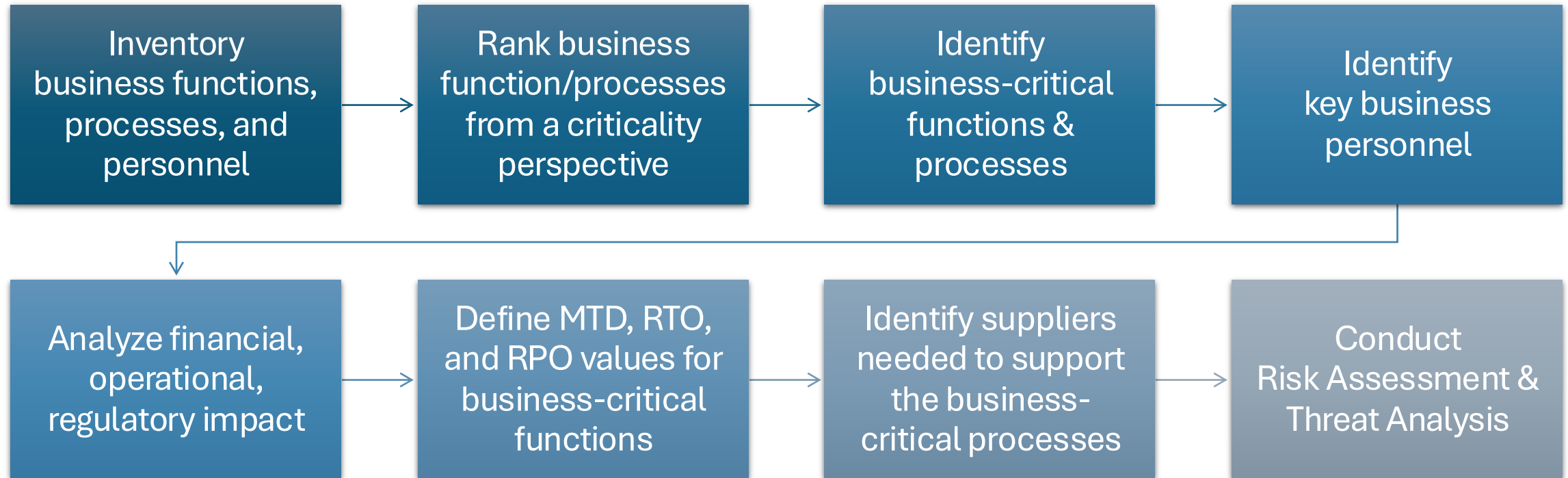
- Perform interviews with stakeholders, analyze assets and threats, quantify risk and conduct risk assessment following the NIST SP 800-34, Rev 1 template

Objective:

- Provide the foundation for a future business continuity plan by identifying and prioritizing critical business functions, processes, and assets



Business Continuity Team's Assessment Approach



Organizational Chart

 = Key Personnel



Information Technology



Finance



Operations



Legal

OWNER

Bill Thomson
Director of IT
Applications

Jass Restrepo
Director of
Service
Delivery

Michael Tran
Director of
Infrastructure
Services

Mike Tyson
CISO

Tom Levy
Director of
Finance and
Accounting

Peter Jenkin
Director of
Operations

Mateo Moss
Director of
Legal
Compliance

SUPPORTING STAFF

Steven Jonhson
Cloud Computing &
Storage Manager

Tracy Davis
SaaS
Applications
Manager

Lena Ortiz
Service Desk
Manager

Leon Kim
Network
Engineer

**Chris
Columbus**
Compliance
Officer

Steven Goldey
Accounting
Manager

Teresa Mendez
Service
Fulfillment and
Delivery

Jenifer Miller
Contractual
Obligations
Council

James Wu
Cloud Engineer

Liam Chen
DevOps
Engineer

Jake Kim
Monitoring &
NOC
Manager

Liam Brooks
System
Administrator

Nelson Mandel
Cybersecurity
Engineer

Sandra Benzo
AP & AR
Manager

Roger Brown
Sales and
Customer
Relations

Hayden Brooks
Compliance
Systems
Council

Anna Patel
Cloud Storage
Administrator

Tara McMillan
SaaS Support
Engineer

Maya Chen
Backup & DR
Services
Manager

Ted Williams
IT Support
Analysts

Winston Scott
Security
Analyst

Tania Garsa
Payroll
Manager

Daniel Browdy
Financial
Reporting
Analyst

Eric Shaw
Change
Management
Manager


Process Stakeholders and Users

Function	Resource	Contact Info	Role	Skill
Cloud Computing	James Wu	jwu@summittech.com	Cloud Engineer	Executes on cloud strategy, operational oversight, and SLA compliance. Expert in VM orchestration on Azure and AWS. Deploy, configure, and troubleshoot virtual machines and storage on cloud platforms to ensure service delivery and optimization.
Cloud Computing	Anna Patel	apatel@summittech.com	Cloud Storage Admin	Domain experts in VM orchestration and storage management. SAN/NAS storage and backup systems (NetApp ONTAP, BackupExec)
Infrastructure	Leon Kim	lkim@summittech.com	Network Engineer	Designs and manages secure network operations
Infrastructure	Liam Brooks	lb Brooks@summittech.com	System Administrator	Managers servers, virtual machines, backups, and patching. Monitor infrastructure health, manage incidents, and maintain availability of hosted services via proactive resource provisioning.
Infrastructure	Ted Williams	twilliams@summitttech.com	IT Support Analyst	Provides support for infrastructure-related incidents and assists in implementing infrastructure changes
Cybersecurity	Chris Columbus	ccolumbus@summittech.com	Compliance Officer	Defines and enforces security standards and strategies
Cybersecurity	Nelson Mandel	nmandel@summittech.com	Cybersecurity Engineer	FedRAMP, NIST, PCI, HIPPA
Cybersecurity	Winston Scott	wscott@summittech.com	Security Analyst	Monitor threats, perform assessments and penetration testing
SaaS Delivery	Liam Chen	lchen@summittech.com	DevOps Engineer	Delivers secure, scalable, and efficient software as a service environments. Leverage cloud VMs and storage for application development, continuous integration, testing, and agile deployment pipelines.




Process Stakeholders and Users

Function	Resource	Contact Info	Role	Skill
SaaS Delivery	Tara McMillan	tmcmillan@summittech.com	SaaS Support Engineer	Resolves customer issues, deploys application updates, monitoring system health and compliance with SLAs and uptime guarantees.
Finance	Sandra Benzo	sbenzo@summittech.com	AP and AR Manager	Ensures cash flow continuity by processing payments of vendor bills and customer's service fees
Finance	Tania Garsa	tgarsa@summittech.com	Payroll Manager	Compensation processing essential for employee retention and legal compliance
Finance	Daniel Browdy	dbrowdy@summittech.com	Financial Reporting Analyst	Business financial performance reporting needed for compliance and stakeholder confidence
Operations	Teresa Mendez	tmendez@summittech.com	Service Fulfillment and Delivery	Tracks fulfillment timelines, performance indicators, and escalates when risk of SLA breach arises. Builds trust and rapport during post-sale service delivery.
Operations	Roger Brown	rbrown@summittech.com	Sales and Customer Relations	Ensures income and customer retention. Understands client needs and tailors solutions rather than pushing generic offerings. Uses CRM tools to track leads, deals, and follow-ups.
Legal	Jenifer Miller	jmillier@summittech.com	Contractual Obligations Council	Reviewing, negotiating, and enforcing contracts to ensure the organization meets its obligations and avoids legal risk
Legal	Hayden Brooks	hbrooks@summittech.com	Compliance Systems Council	Focused on systems and regulatory infrastructure (e.g., GDPR, HIPAA, SOX, CCPA, FISMA) to provide interpretation and ensure adherence

Critical Functions/Process

Core Service	Function	Process	Required Resource	Resource Detail	Location	Process Description
 IT Infrastructure Management	Infrastructure Services	Remote Access Management	<ul style="list-style-type: none"> VPN Server Endpoint client MFA RBAC 	<ul style="list-style-type: none"> Firepower/AnyConnect Secure Mobility Client 	Hybrid (On-premise + Cloud-based)	Delivers secure, policy-driven connectivity for employees and partners accessing company systems from external networks. It supports continuous, compliant service delivery by enforcing encryption, authentication, and role-based access controls (RBAC).
	Service Delivery	Remote Monitoring and Management	<ul style="list-style-type: none"> RMM tool Firewalls Routers Switches Wireless 	<ul style="list-style-type: none"> ConnectWise RMM 	Cloud	Ensures reliable connectivity across company operations by actively managing the performance and availability of the company's network infrastructure. This process plays a critical role in supporting day-to-day business functions by maintaining consistent access to systems, services, and communication channels .
	Service Delivery	Backup & Recovery	<ul style="list-style-type: none"> Backup Server 	<ul style="list-style-type: none"> Veeam 	On-premise	Ensures that critical systems and cloud-based applications, such as Microsoft 365, are regularly backed up and recoverable. This supports business continuity, regulatory compliance, and rapid restoration in the event of data loss or service disruption.

Critical Functions/Process

	Core Service	Function	Process	Required Resource	Resource Detail	Location	Process Description
	SaaS-based enterprise software	Finance and Accounting	Payroll	<ul style="list-style-type: none"> ERP Payroll Module 	<ul style="list-style-type: none"> SAP S/4HANA Cloud 	Cloud	Oversees the accurate and timely administration of employee compensation , salaries, bonuses, and commissions, based on validated time, performance, and contractual obligations. This directly supports regulatory compliance , employee trust , and uninterrupted business operations .
	SaaS-based enterprise software	Operations	Sales and Customer Relations	<ul style="list-style-type: none"> CRM 	<ul style="list-style-type: none"> Salesforce CRM 	Cloud	Encompasses the methods to build and maintain relationships with its customers , fostering loyalty and satisfaction . It involves understanding customer needs, providing support, and ensuring a positive overall experience.
	SaaS-based enterprise software	Legal Compliance	Contractual Obligations Compliance	<ul style="list-style-type: none"> CRM 	<ul style="list-style-type: none"> Salesforce to DocuSign Contract Lifecycle Management (CLM) Integration 	Cloud	Ensures adherence to laws, regulations, industry standards , and internal policies to prevent misconduct and maintain legal compliance across areas such as employment law, environmental compliance, and data protection.

Key Personnel Inventory

Function	Resource	Contact Info	Role	Skill
SaaS Delivery	Tracy Davis	tdavis@summittech.com	SaaS Applications Manager	Leads SaaS deployment and integration for critical systems (ERP/CRM); downtime or misconfiguration would halt user access and disrupt business operations.
IT	Jake Kim	jkim@summittech.com	Monitoring & NOC Manager	Ensures uptime for remote access and internal infrastructure. Key to early threat detection and service stability.
Finance	Tania Garsa	tgarsa@summittech.com	Payroll Manager	Owns the payroll process using ERP. Failure here would result in missed compensation and regulatory penalties.
IT	Leon Kim	lkim@summittech.com	Network Engineer	Supports secure remote access (VPN, MFA, RBAC). Critical for enabling 75% of remote staff and maintaining compliance.
IT	Maya Chen	mchen@summittech.com	Backup & DR Services Manager	Oversees backup integrity and recovery, essential for disaster recovery and compliance with RPO/RTO metrics.
Legal	Jenifer Miller	jmiller@summittech.com	Contractual Obligations Council	Ensures legal compliance and risk avoidance through vendor and contract oversight, crucial for avoiding regulatory breaches.

Business Function/Process Impact

Core Service/Function	Process	Impact Description	Financial Cost	Operational	Regulatory
IT/Infrastructure	Remote Access/VPN	Disruption in VPN access would prevent remote employees (75% of workforce) from connecting to internal systems	\$50,000/hour	High	High
IT/Service Delivery	Remote Monitoring and Management	Outage would leave the organization blind to system health and unable to respond to incidents	\$40,000/hour	High	High
IT/Service Delivery	Backup & Recovery	Loss of backup and recovery services would prevent data restoration after an incident, increasing the risk of permanent data loss and prolonged downtime, severely affecting business continuity	\$100,000/hour	High	High
SaaS/Finance	Payroll	If payroll systems are down, employee pay is delayed, leading to legal risk and loss of trust	\$30,000/hour	High	High
SaaS/Customer Relations	Sales and Customer Relations	CRM outage impacts sales, customer service, and relationship management, resulting in revenue loss and churn	\$45,000/hour	High	High
SaaS/Compliance	Contractual Obligations Compliance	Delayed access to legal documentation and audit records can result in non-compliance with regulations	\$25,000/hour	High	High

Business Function/Process Recovery Metrics

Function	Process	Required Resource	MTD	RTO	RPO
Infrastructure Services	Remote Access Management	VPN server, Endpoint client, MFA. RBAC	24 hours	12 hours	15-30 min
Service Delivery	Remote Monitoring & Management	RMM tool, firewalls, switches, routers, wireless	24 hours	12 hours	15-30 min
Service Delivery	Backup & Recovery	Backup Server	12 hours	6 hours	15 min
Finance & Accounting	Payroll	ERP Payroll Module	48 hours	36 hours	1 hour
Operations	Sales & Customer Relations	CRM	24 hours	12 hours	1 hour
Legal Compliance	Contractual Obligations Compliance	CRM	48 hours	36 hours	24 hours

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

IT Suppliers Requiring Use of SummitTech Functions

Function	Resource Detail	Affected Users	How Supplier Uses This Function
Secure Remote Access	Cisco Firepower/AnyConnect Secure Mobility Client	Company & Client	Suppliers require SummitTech's secure and stable remote access solutions, enabling external teams and partners to safely and consistently access necessary resources remotely.
Remote Monitoring & Management	ConnectWise RMM	Company & Client	Suppliers depend on SummitTech's comprehensive remote monitoring to proactively detect and resolve system issues, preventing service disruptions affecting their own customers.
Data Backup & Recovery	Veeam Backup & Replication	Company & Client	Suppliers rely heavily on SummitTech's robust backup solutions to protect critical client data and ensure quick, reliable restoration to maintain continuous service operations.

Enterprise Software Suppliers Requiring Use of SummitTech Functions

Critical Function	Function	Resource Detail	Affected Users	How Supplier Uses This Function
Finance	ERP - Payroll Processing	SAP S/4HANA ERP	Company	Suppliers depend on SummitTech's accurate and timely payroll processing to reliably manage payments to contractors, vendors, and maintain financial stability.
Operations	CRM - Sales & Service Modules	Salesforce CRM	Company	Suppliers rely on SummitTech's CRM for precise, real-time sales and support information critical to effective collaboration, streamlined client management, and customer satisfaction.
Legal	Contract Lifecycle Management	Salesforce & DocuSign CLM Integration	Company	Suppliers count on SummitTech's integrated contract management solution to streamline contract creation, review, and execution processes, minimizing compliance risks and operational delays.

Threat Analysis and Risk Assessment



Step 1. Risk Identification

Asset Assessment

Asset Name	Criterion 1: Impact on Regulatory Compliance	Criterion 2: Impact on Revenue/ Profitability	Criterion 3: Impact on Public Image	Criterion 4: Impact on Operations	Weighted Score
Criterion Weight (1-100)	30	40	20	10	100
Veeam	0.8	0.9	0.9	0.8	86
ConnectWise RMM	0.7	0.8	0.7	0.9	76
Cisco Firepower/AnyConnect Secure Mobility Client	0.9	0.8	0.8	0.9	84
SAP S/4HANA ERP	0.9	0.9	0.9	0.9	90
Salesforce	0.8	0.9	0.6	0.6	78
Salesforce to DocuSign CLM Integration	0.9	0.6	0.8	0.7	74

Step 2. Threat Assessment

Threat Event: Cyber Attack (DDoS, Ransomware)

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

Threat Assessment (continued)

Threat Event: Data Breach

Asset Name	Asset Location	Vulnerability	Impact	Probability	Severity	Risk Factor	Mitigation
Veeam	On-premise	Improper access control on backup files	Exposure of sensitive backup data	3	5	15	Encrypt backup files, restrict access, log access attempts
ConnectWise RMM	Cloud	Credential leaks or insecure API tokens	Unauthorized control over remote systems	4	5	20	Secure API keys, enforce token expiration, MFA
Cisco Firepower/ AnyConnect Secure Mobility Client	On-premise	Misconfigured firewall rules or insecure VPN policies	Unauthorized access to internal network	3	4	12	Review firewall rules, enforce strong VPN access controls
SAP S/4HANA ERP	Cloud	Access to sensitive business data through misconfigured roles	Leak of financial and customer transaction data	4	5	20	Use least privilege roles and encryption-at-rest
Salesforce	Cloud	Weak user permissions or shared credentials	Breach of customer data and analytics insights	3	4	12	Enforce role-based access, remove unused users, enable MFA
Salesforce to DocuSign CLM Integration	Cloud	Insufficient API protection and identity verification	Disclosure of signed legal agreements or contract data	3	5	15	Use secure integration tokens, enable logging, verify user identity

Threat Assessment (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	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

Threat Assessment (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		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

Threat Assessment (continued)

Threat Event: Misconfiguration

Asset Name	Asset Location	Vulnerability	Impact	Probability	Severity	Risk Factor	Mitigation
Veeam	On-premise	Improper backup job scheduling or retention policies	Loss of backup data or failure to restore properly	4	4	16	Regular configuration audits, role-based scheduling
ConnectWise RMM	Cloud	Open ports or unsecured remote connections	System compromise through RMM console	4	5	20	Harden system settings, disable unused ports
Cisco Firepower/AnyConnect Secure Mobility Client	On-premise	Incorrect firewall rules or weak encryption settings	Exposed VPN or firewall allowing unauthorized access	3	4	12	Periodic firewall review and validation
SAP S/4HANA ERP	Cloud	Unrestricted roles or unpatched services	Unauthorized changes or data leakage	4	5	20	Security baselines, enforce patch and role reviews
Salesforce	Cloud	Over-permissive data sharing and app integrations	Breach of sensitive sales or customer records	3	4	12	Access governance, restrict API use, validate app settings
Salesforce to DocuSign CLM Integration	Cloud	Misconfigured tokens or webhook exposure	Unauthorized access to contract workflows or metadata	3	5	15	Secure integration policies, verify token scopes, enable logs

Application of AI in This Project

Throughout our Business Impact Analysis (BIA) and Risk Assessment for SummitTech Solutions, we used AI tools (e.g., ChatGPT from OpenAI) to help guide our research, structure content, and provide relevant examples.

Slide 2 – SummitTech's Business Objectives

- AI helped generate clear, realistic business objectives for a \$750M cybersecurity-focused SaaS provider.

Slides 4-5 - Core Services & BIA Methodology

- Provided examples for core managed services (ERP, CRM, cybersecurity consulting).
- Suggested best practices for conducting our Business Impact Analysis.

Slides 7-9 - Organization & Stakeholders

- Helped define roles clearly for positions like Network Engineer, Cybersecurity Analyst, and SaaS Manager.

Application of AI in This Project

Slides 10-12 - Critical Functions & Key Personnel

- Offered industry-standard descriptions for critical processes like Remote Access Management, Backup Services, and Monitoring & NOC operations.

Slides 13-14 - Business Impact & Recovery Objectives

- Assisted with benchmarking recovery metrics like MTD, RTO, and RPO, ensuring realistic continuity planning.

Slides 15-16 - IT Services & Suppliers

- Provided concise descriptions for critical systems including Veeam, CiscoFirepower, ConnectWise, and SAP ERP.

Slides 17-19 - Threat Assessment & Risk Identification

- Supplied practical examples of vulnerabilities and threats affecting backups, ERP, and CRM systems.
- Suggested realistic and effective mitigation strategies.