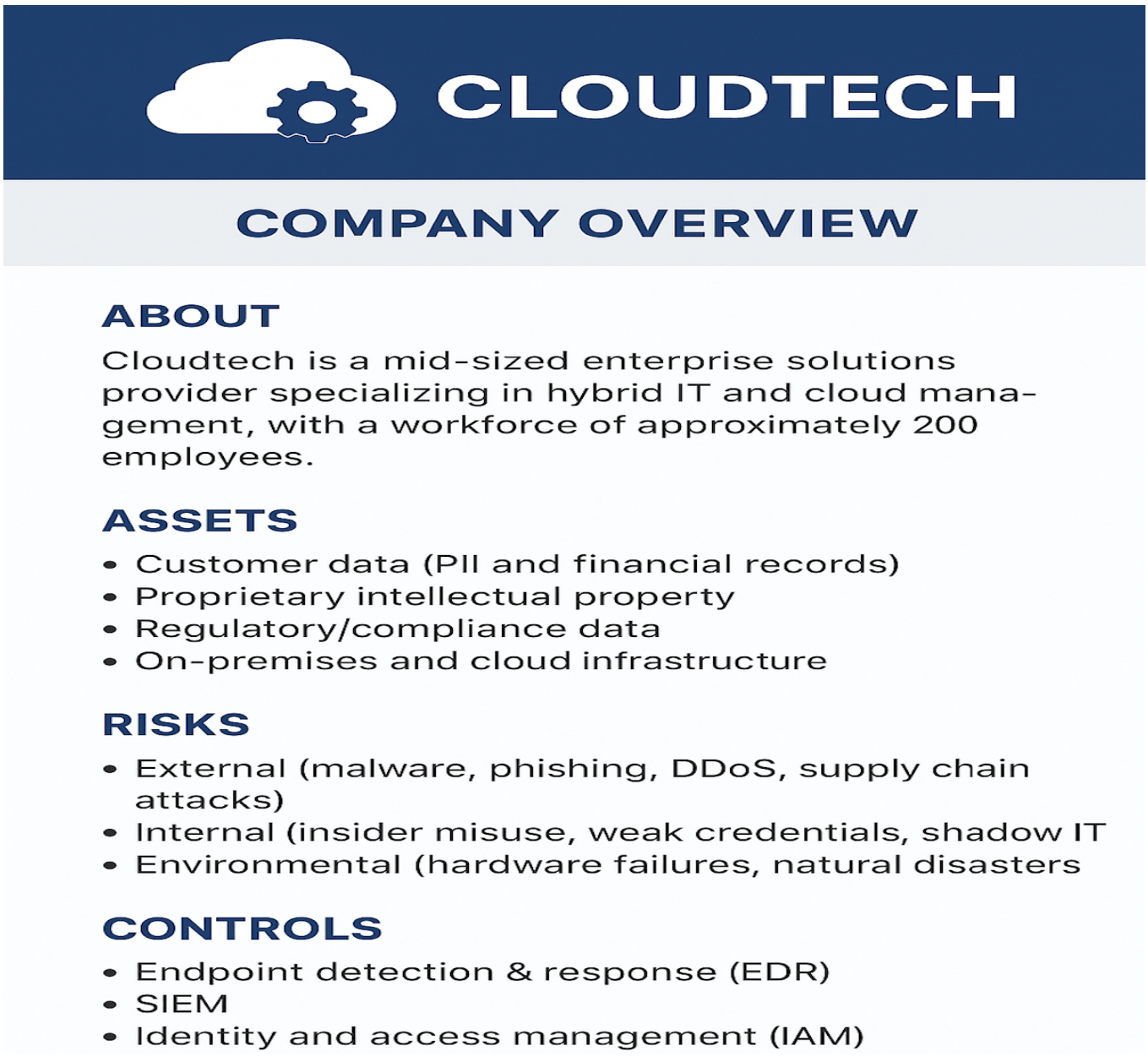
Cloud tech Enterprise Risk Assessment Simulation

Prepared By: Purna Kishore Kondapaneni |



Cloud tech Enterprise Risk Assessment Simulation

Table of Contents

1. **Executive Summary**
2. **Introduction**
3. **Company Overview**
4. **Major IT Assets**
    - Hardware
    - Software
    - Data
5. **Threat Catalog**
    - External Threats
    - Internal Threats
    - Operational/Environmental Threats
6. **Risk Assessment (Impact & Likelihood)**
7. **Mitigation Strategies & Controls**
8. **Conclusion & Recommendations**

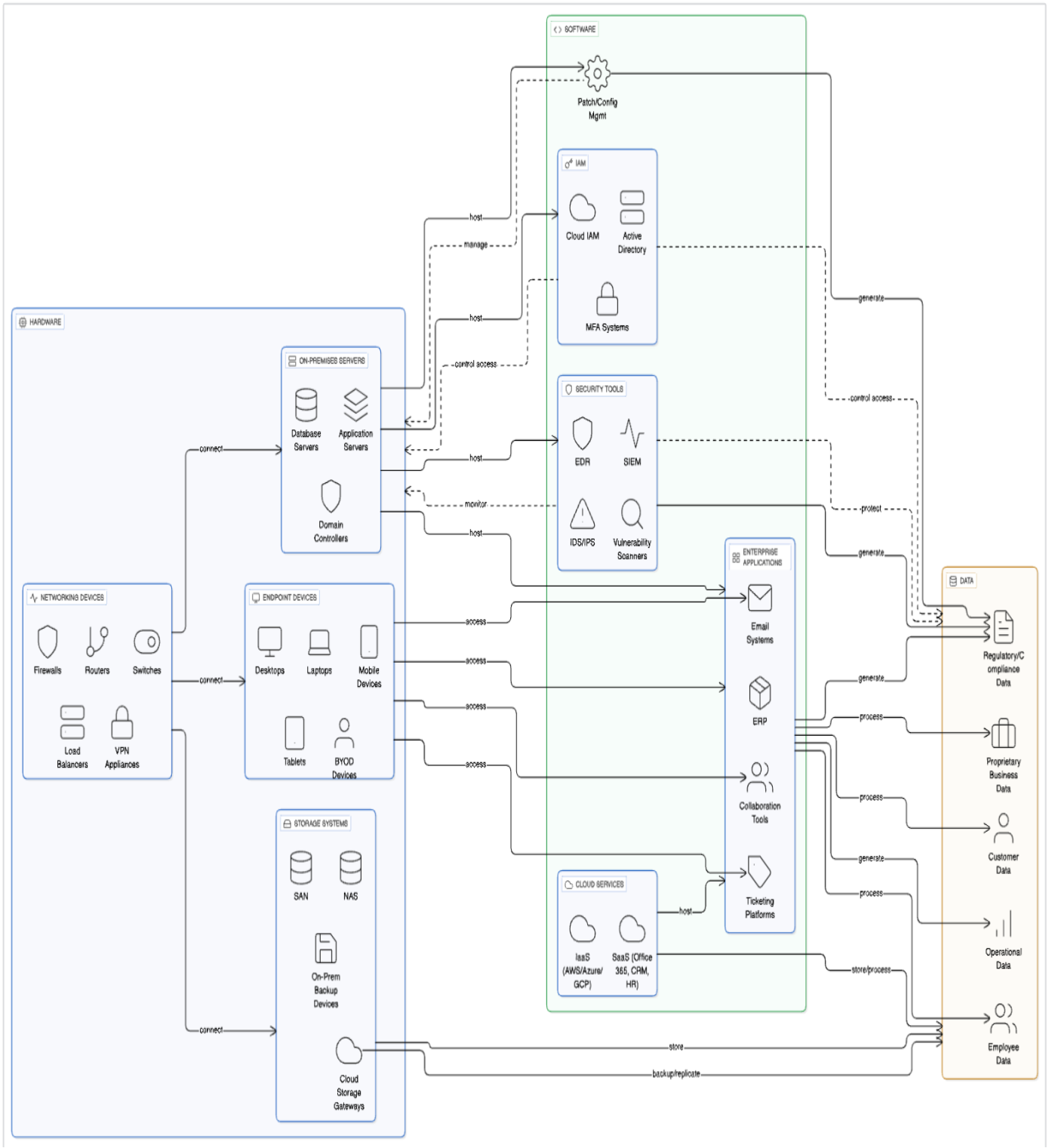
Executive Summary

Cloud tech manages a complex hybrid environment supporting endpoint devices both on-premises and in the cloud. This raises significant security considerations as sensitive data flows across multiple platforms and devices. Recently conducted risk assessments have identified vulnerabilities that risk the confidentiality, integrity, and availability (CIA) of critical systems. Immediate and proactive mitigation strategies are recommended to address unpatched systems, weak authentication, insecure communications, and insider risks. This report summarizes key risks, their potential impacts on business operations, and prioritized mitigation recommendations essential to safeguarding company assets and ensuring compliance.

Figure 1 shows the Typical Enterprise environment Infrastructure:

Cloud tech Enterprise Risk Assessment Simulation

Enterprise IT Asset Environment Overview



Cloud tech Enterprise Risk Assessment Simulation

1. Major IT Assets

Hardware

- **On-Premises Servers** (databases, application servers, domain controllers)
- **Networking Devices** (firewalls, routers, switches, load balancers, VPN appliances)
- **Endpoint Devices** (desktops, laptops, mobile devices, tablets – including BYOD)
- **Storage Systems** (SAN/NAS, on-prem backup devices, cloud storage gateways)

Software

- **Cloud Services** (IaaS platforms like AWS/Azure/GCP, SaaS apps like Office 365, CRM, HR systems)
- **Enterprise Applications** (ERP, collaboration tools, email systems, ticketing platforms)
- **Security Tools** (endpoint detection & response (EDR), SIEM, IDS/IPS, vulnerability scanners)
- **Identity & Access Management (IAM)** (Active Directory, cloud IAM, MFA systems)
- **Patch and Configuration Management Tools**

Data

- **Customer Data** (PII, financial records, contracts, client communications)
- **Proprietary Business Data** (intellectual property, internal research, trade secrets)
- **Operational Data** (log files, monitoring data, usage metrics, system configurations)
- **Employee Data** (HR records, payroll, personal information)
- **Regulatory/Compliance Data** (audit reports, legal/financial documents.

Cloud tech Enterprise Risk Assessment Simulation

Risk Management Process in the Enterprise Environment

NIST describes the risk management process as a cycle with four key components:

1. Frame Risk: Establish the context, including defining business objectives, regulatory requirements, and risk appetite.
2. Assess Risk: Identify threats, vulnerabilities, and internal/external risk factors that could negatively impact information systems. Evaluate both the likelihood and potential impact of these risks.
3. Respond to Risk: Develop and implement mitigation, transfer, acceptance, or avoidance strategies for assessed risks.
4. Monitor Risk: Continuously monitor risks and controls to address any changes in the threat or business environment.

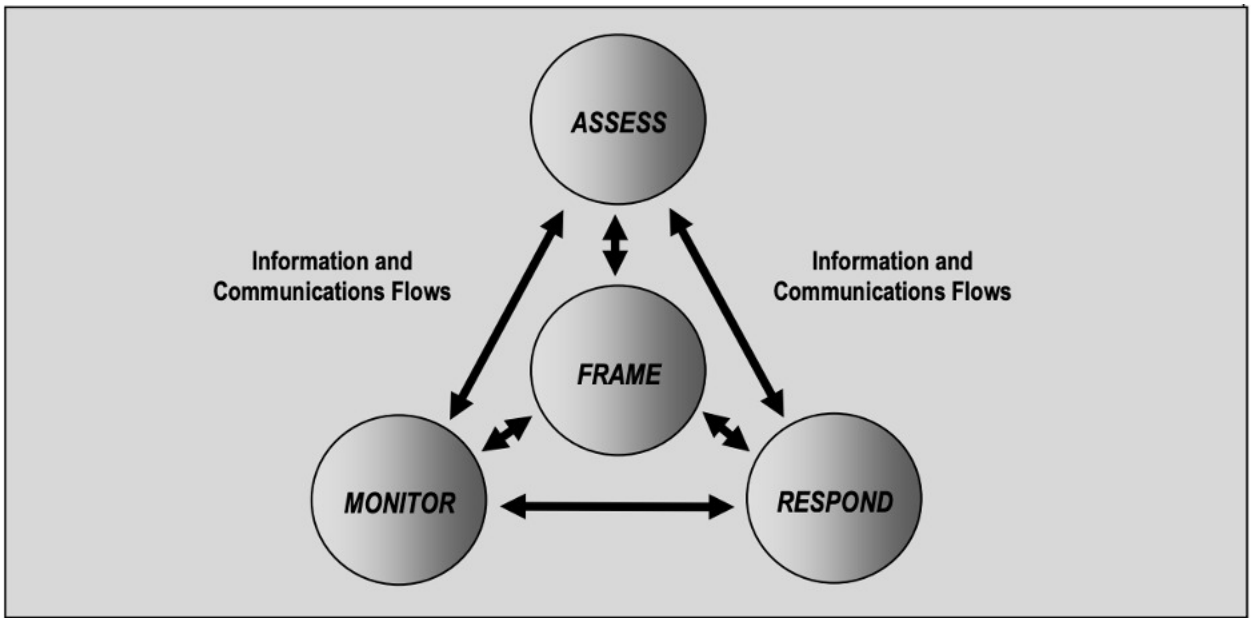


Figure 2: RISK MANAGEMENT PROCESS

Cloud tech Enterprise Risk Assessment Simulation

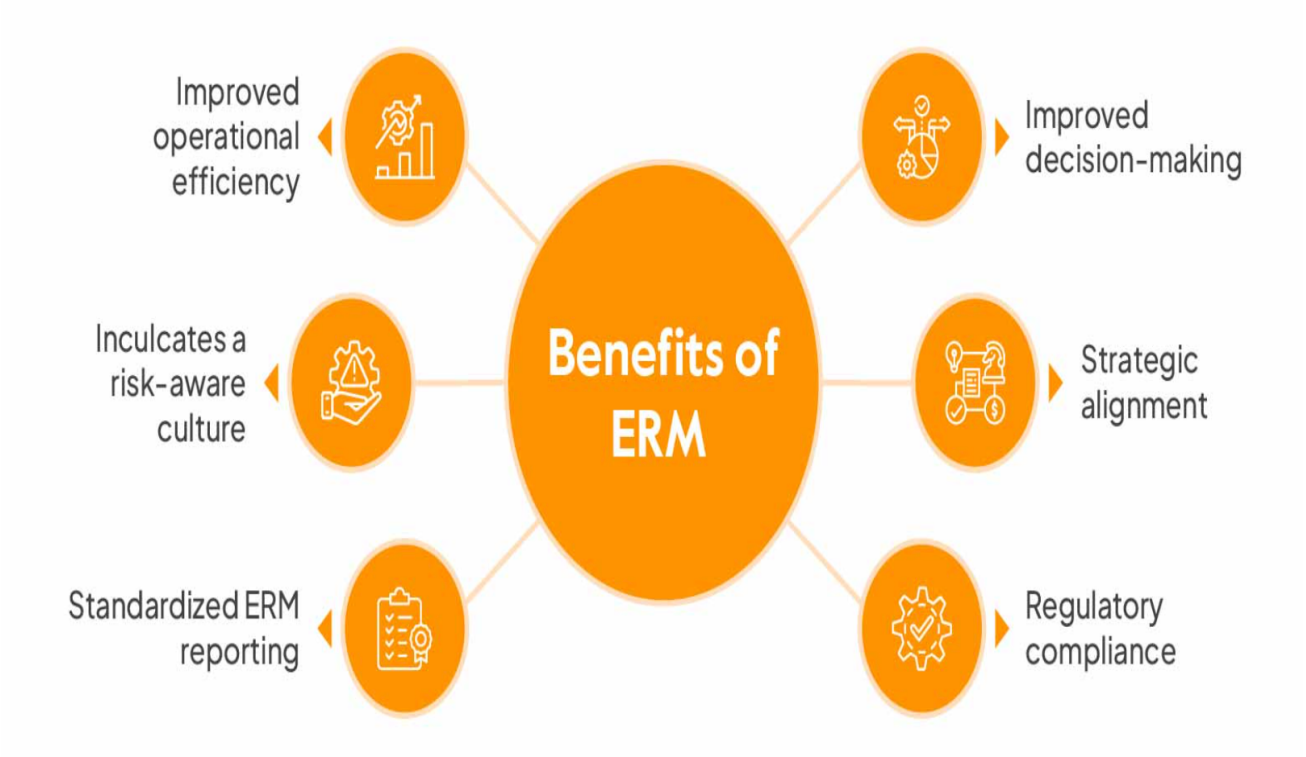
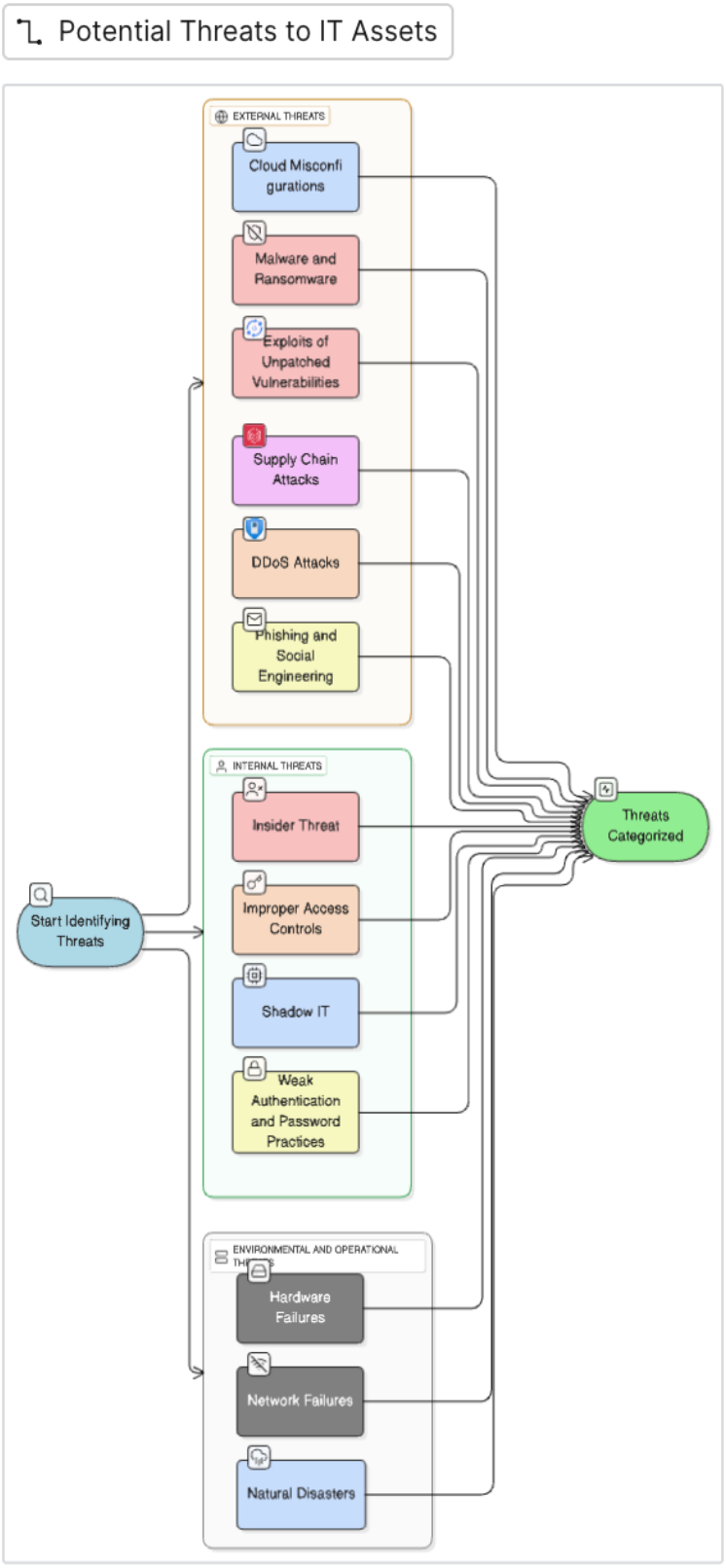


Figure 3: Benefits of Enterprise Risk Management

Potential Threats for ERM Assets:

External Threats	Internal Threats	Environmental Threats
Malware, phishing, DDoS, unpatched vulnerabilities, cloud misconfigurations, supply chain attacks	Insider misuse, weak passwords, shadow IT, poor access controls	Hardware failures, natural disasters, network outages

Cloud tech Enterprise Risk Assessment Simulation



External Threats:

- **Malware & Ransomware** – Exploiting unpatched systems, encrypting data for ransom
- **Phishing & Social Engineering** – Credential theft, account compromise
- **DDoS Attacks** – Targeting servers or cloud services to disrupt availability
- **Exploits of Unpatched Vulnerabilities** – Remote code execution, privilege escalation
- **Cloud Misconfigurations** – Exposed storage buckets, overly permissive IAM roles
- **Supply Chain Attacks** – Compromised third-party software updates

Internal Threats:

- **Insider Threat (Malicious or Negligent Employees)** – Data theft, sabotage, unintentional errors
- **Weak Authentication/Password Practices** – Shared accounts, default credentials
- **Shadow IT** – Unauthorized apps or devices connecting to the network
- **Improper Access Controls** – Excessive privileges, lack of role-based access

Environmental/Operational Threats:

- **Hardware Failures** – Disk crashes, power supply issues
- **Natural Disasters** – Fire, flood, power outage impacting on-prem data centers
- **Network Failures** – Connectivity issues disrupting cloud/on-prem hybrid workflows

Cloud tech Enterprise Risk Assessment Simulation

Key Areas for Security Assessment:

- Identifying Risk Assets: Inventory and categorize all devices, data repositories, and systems.
- User Authentication & Credentials: Assess the strength of authentication methods (e.g., MFA) and account management processes.
- Software Update and Patch Management: Examine how vulnerabilities are mitigated through timely update and patch processes.
- Cloud Security & Hardening: Evaluate cloud infrastructure for security configuration, segmentation, and exposure.
- Encryption & Data Protection: Review at-rest, in-transit, and backup data protection mechanisms along with following GDPR rules in Europe region.
- Access Control & Monitoring: Scrutinize privilege assignments, segregation of duties, and continuous logging of access/activity.
- Supply Chain Management: Evaluate vendor security practices and third-party integrations.
- Employee Training and Insider Threat Awareness: Assess ongoing awareness and education initiatives for staff.

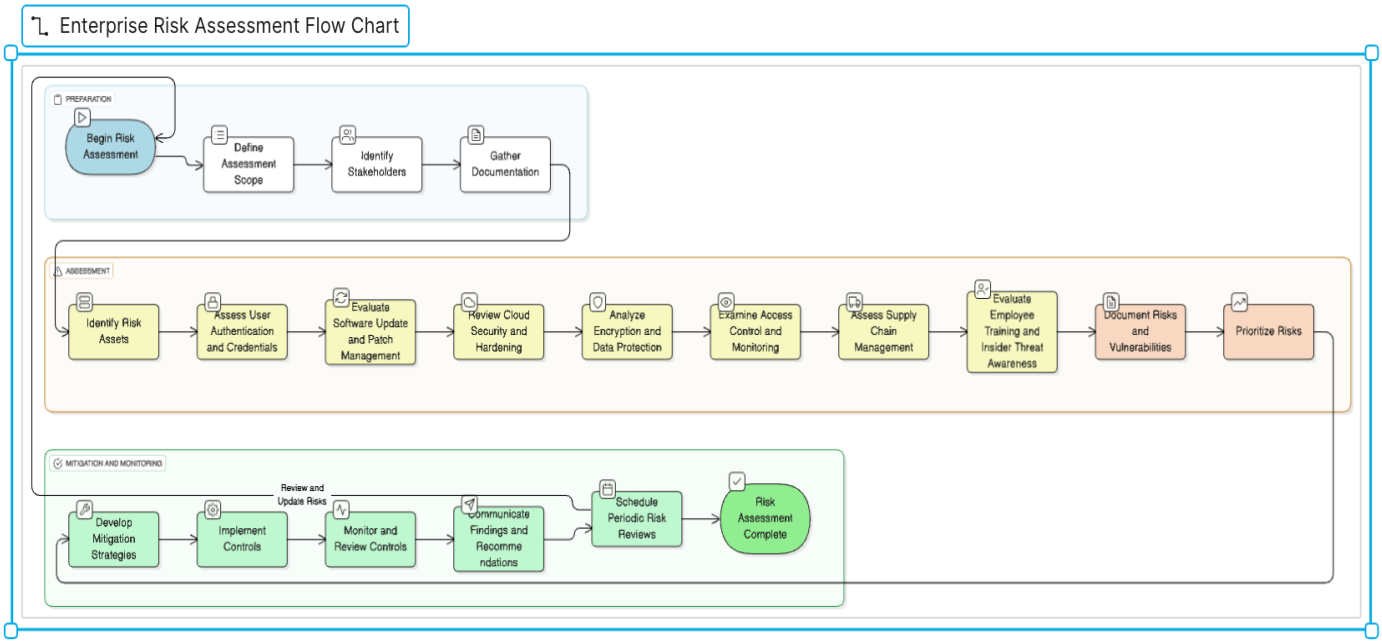


Figure 4: Components of Enterprise Risk Management along with process of assessment

Cloud tech Enterprise Risk Assessment Simulation

NIST 800-30: Core Risk Assessment Steps

1. Prepare for Assessment: Define the system scope and assemble documentation, user profiles, and asset inventories needed for analysis:
2. Identify Threats and Vulnerabilities: Document possible threat actors and events (e.g., hackers, malware, misconfiguration) and identify system vulnerabilities.
3. Determine Likelihood and Impact: For each risk scenario, estimate the probability of occurrence and the magnitude of impact on organizational operations, assets, and individuals.
4. Calculate and Prioritize Risks: Assign a risk level by combining likelihood and impact and prioritize high risks for mitigation.
5. Document and Communicate Results: Clearly report findings to stakeholders, supporting risk-informed decision making.
6. Monitor and Update: Continuously monitor risk factors, update risk assessments as situations evolve, and verify control effectiveness.

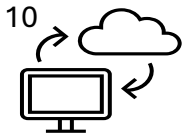
Application to Cloud tech

Given Cloud tech’s hybrid context, risk assessment must account for:

- Data movement between on-premises and cloud systems.
- Device diversity and exposure to BYOD risks.
- The speed of threat evolution vs. patching and control deployment.
- Regulatory and contractual requirements involving client data.

A robust, repeatable assessment process (as outlined in NIST 800-30 and NIST RMF) ensures continuous protection for critical systems and business operations.

To conduct a vulnerability analysis in a company's network like Cloud tech, simple tools and hypothetical scenarios can be used to identify and document risks such as unpatched software or weak passwords. Here’s a practical approach:



Cloud tech Enterprise Risk Assessment Simulation

Conducting Vulnerability Analysis

1. Select and Use of Vulnerability Scanning Tools

- Start with tools like OpenVAS (open source), Nessus, or Qualys VMDR for network and endpoint scanning.
- Tools scan for weaknesses like outdated software, misconfigurations, or missing patches, and often include checks for weak credentials.
- Free tools such as Nmap (with security scripts) and ZAP (for web apps) are also effective for small environments or targeted tests.

2. Hypothetical Scenarios

- If full automation is not possible, create “what-if” cases: e.g., consider if an attacker exploited a known, unpatched vulnerability in a device; or if employee passwords are easily guessable.
- Analyze what could happen in each scenario and which systems or data would be impacted.

3. Document Vulnerabilities

- For each identified vulnerability (from automated scans or scenarios), record:

- Description: What is the flaw? (e.g., “Windows server missing June 2025 security update” or “admin passwords are set to default values”)
- Potential Impact: What could go wrong? (e.g., “Ransomware infection,” “Data theft,” “Denial of Service”)
- Likelihood: Use qualitative ratings (High/Medium/Low) based on exploitability and exposure or use a scoring system like CVSS.
- Mitigation: Note recommended fixes (install patch, enforce password policy, etc.)

4. Prioritize Remediation

- Focus on vulnerabilities with both high impact and high likelihood first (e.g., unpatched remote code execution flaws, weak cloud credentials).

5. Reporting

Cloud tech Enterprise Risk Assessment Simulation

- Produce a summary report linking vulnerabilities to their business impact and remediation urgency.

Vulnerability	Impact	Likelihood	Recommended Action
Unpatched web server	Data breach	High	Apply latest patches
Weak admin password	Data loss	High	Enforce strong password policy
Outdated endpoint agent	Service outage	Medium	Update endpoint software

This approach helps make vulnerability analysis structured and actionable, even for organizations just starting with security assessments.

For hybrid endpoints - devices managed across both cloud and on-premises environments, the highest priority risks to treat often include:

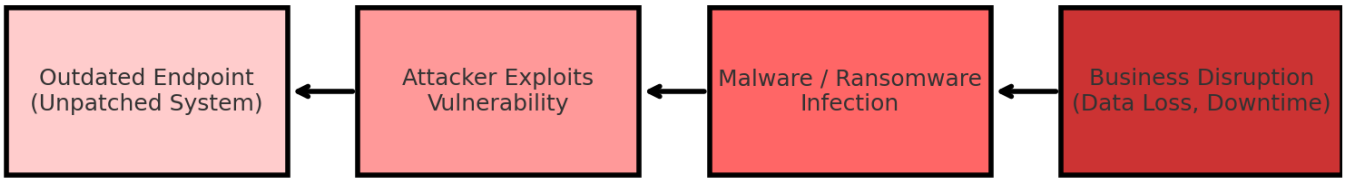
High Priority Risks for Hybrid Endpoints

Risk	Scenario	Impact	Fix
Unpatched Vulnerabilities	A company laptop hasn't installed the latest Windows update. A ransomware campaign exploits this and encrypts files across the network.	Data loss, downtime, and ransom demand.	Enable automatic updates, patch critical vulnerabilities quickly.
Weak or Compromised Credentials	An employee reuses a weak password for personal and work accounts. Attackers use stolen credentials to log into the cloud portal.	Unauthorized access to sensitive systems.	Enforce strong passwords and multi-factor authentication (MFA).
Insecure Communication Channels	A remote worker uploads files over unsecured Wi-Fi without VPN. Hackers intercept	Confidential data interception and leakage.	Mandate VPN, TLS encryption, and secure Wi-Fi connections.

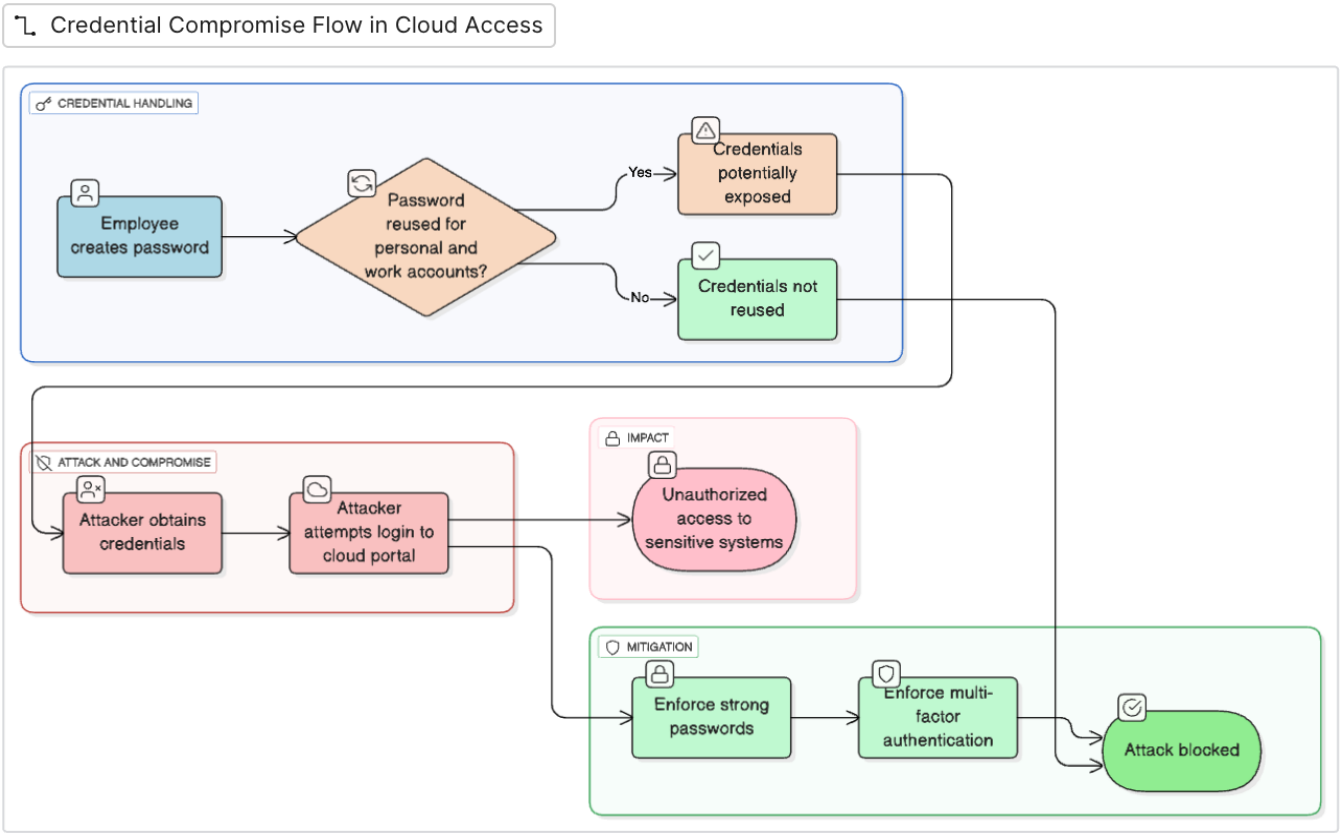
Cloud tech Enterprise Risk Assessment Simulation

	traffic and steal documents.		
Misconfigured Endpoint Management Tools	IT forgets to restrict admin rights in a management tool. An attacker pushes malicious updates to all company devices.	Widespread malware infection across endpoints.	Apply least-privilege principle and regularly audit tool settings.
Shadow IT and Unmanaged Devices	An employee connects a personal USB drive that carries malware, infecting the system and leaking data.	Malware infection, data leakage, bypass of security controls.	Block unauthorized devices and monitor for shadow IT.
Insider Threat and Lack of User Awareness	A staff member clicks a phishing email disguised as a payroll update, installing spyware that steals login credentials.	Account compromise and potential data breach.	Conduct security awareness training and phishing simulations.
Supply Chain Risks	A third-party software update is compromised with backdoor malware, spreading through the company's endpoints.	Unauthorized remote access and data theft.	Vet vendors, validate updates, and use code-signing verification.

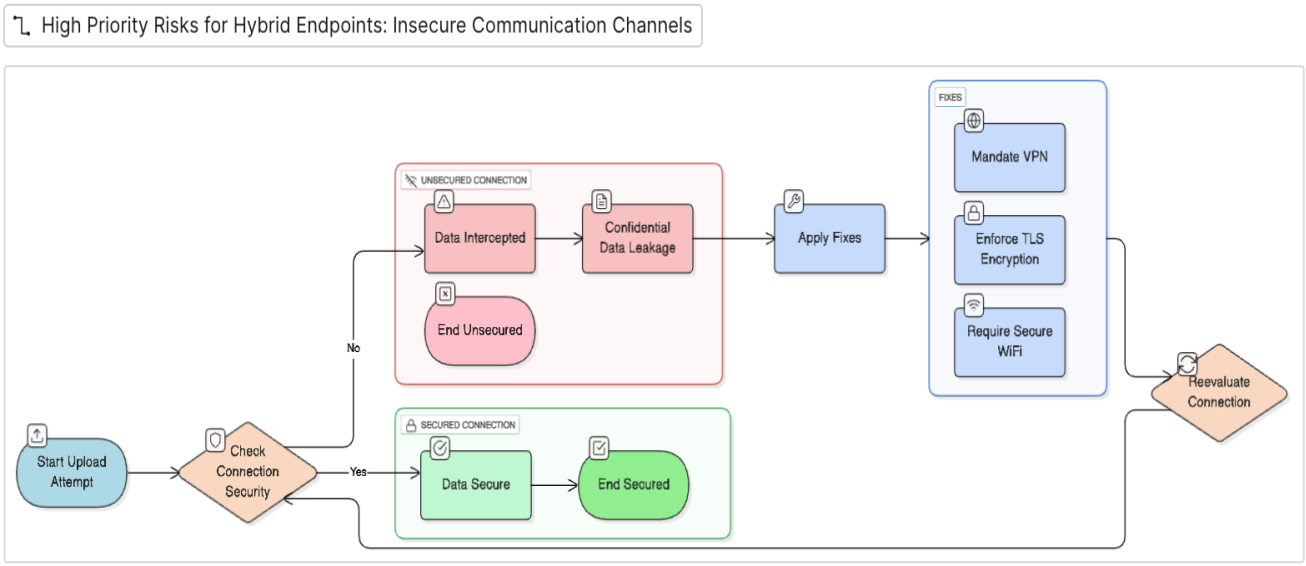
For Unpatched vulnerabilities scenario path:



Cloud tech Enterprise Risk Assessment Simulation



For weak compromised passwords & Insecure communication channels path:



Cloud tech Enterprise Risk Assessment Simulation

Summary Table of High Priority Risks

Risk	Reason for High Priority
Unpatched vulnerabilities	Easy exploit leading to widespread endpoint compromise
Weak/compromised credentials	Facilitates unauthorized access
Insecure communication	Allows data interception between cloud & on-premises
Misconfigured endpoint tools	Risk of lateral movement & privilege escalation
Shadow IT/unmanaged devices	Unmonitored entry points for attackers
Insider threat/user error	Human factor often exploited in breaches
Supply chain vulnerabilities	Third-party risk impacting endpoint security

Addressing these risks promptly with layered controls such as patch automation, MFA, encrypted communications, secure configurations, user training, and supply chain vetting will significantly improve security posture for hybrid endpoints.

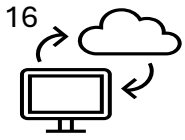
Risk Assessment Findings

Risk Area	Description	Potential Impact	Likelihood	Priority	Recommended Mitigation
Unpatched Software	Devices or servers with missing critical patches	High: Exploitation leading to ransomware or data breach	High	High	Implement automated patch management
Weak Authentication & Credentials	Lack of MFA and poor password practices	High: Unauthorized access, data loss	High	High	Enforce MFA and strict password policies
Insecure Cloud Configurations	Misconfigured cloud platforms exposing data or services	High: Data exposure, compliance issues	Medium	High	Harden cloud setup, use encryption

Cloud tech Enterprise Risk Assessment Simulation

Endpoint Management Misconfiguration	Overly permissive device management settings	Medium: Lateral movement risk	Medium	Medium	Regular audits and hardened configuration
Insider Threat & Awareness	Lack of employee training, risks of phishing and social engineering	Medium: Data leaks or sabotage	Medium	Medium	Conduct ongoing security awareness programs
Supply Chain Vulnerabilities	Vendor security weaknesses impacting endpoint software or devices	Medium: Introduction of vulnerabilities	Low	Medium	Perform vendor security assessments

Enterprise Risk Matrix Based on the Risk



Cloud tech Enterprise Risk Assessment Simulation

Risk Mitigation Plan and Prioritization

1. Immediate (High Priority)
    - Deploy automated patching tools across all endpoints and servers.
    - Enforce multi-factor authentication on critical systems.
    - Harden cloud infrastructure configurations and enforce encryption.
2. Medium Term (Moderate Priority)
    - Conduct regular security audits and endpoint management reviews.
    - Enhance employee training programs focused on security awareness.
    - Establish a vendor risk management and assessment framework.

Here are common enterprise risk mitigation strategies with practical examples:

1. Risk Avoidance

- **Strategy:** Avoid activities that expose the organization to risk.
- **Example:** A healthcare company chooses not to collaborate with a vendor that lacks strong cybersecurity controls, despite potential business benefits, to avoid risk of patient data breach.

2. Risk Reduction

- **Strategy:** Implement controls to reduce the likelihood or impact of risks.
- **Example:** Regular patching of software and systems to close vulnerabilities and reduce chances of malware infection. Enforcing multi-factor authentication (MFA) to prevent unauthorized access.

3. Risk Transference

- **Strategy:** Shift risk responsibility to a third party.
- **Example:** Purchasing cyber insurance to cover financial losses from data breaches or ransomware attacks.

4. Risk Acceptance

- **Strategy:** Acknowledge the risk and decide to accept it when the cost of mitigation outweighs the potential impact.

Cloud tech Enterprise Risk Assessment Simulation

- **Example:** Accepting minor operational delays as part of normal business operations while monitoring their occurrence.

5. Risk Isolation

- **Strategy:** Separate or contain risk to minimize impact on other areas.
- **Example:** Segmenting the network so that critical systems are isolated from public-facing servers, thereby limiting lateral movement if a breach occurs.

6. Risk Buffering

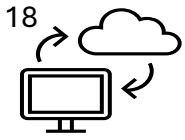
- **Strategy:** Add resources to absorb impact.
- **Example:** Maintaining backup power generators and redundant internet connections to ensure continuity in case of failures.

7. Employee Training and Awareness

- **Strategy:** Equip staff to recognize and respond to risks.
- **Example:** Regular phishing simulations and security awareness training to reduce insider risk and social engineering attacks.

Mitigation Strategies & Controls achieved through Security Controls:

1. Technical Controls	2. Administrative Controls	3. Operational Controls
• MFA on all critical systems • Data encryption (at rest & in transit) • Patch management automation • Endpoint detection & response (EDR) • Cloud security hardening	• Security governance policies • Vendor risk management • Role-based access control (RBAC) • Regular compliance audits • Employee awareness training	• Incident response (IR) plan & tabletop exercises • Backup & disaster recovery drills • Continuous monitoring via SOC • Physical security for servers and devices



Cloud tech Enterprise Risk Assessment Simulation

Implementing these strategies methodically based on risk prioritization helps enterprises reduce exposure while optimizing resource allocation. Risk owners should document the selected approach and review regularly to adapt as the risk landscape evolves.

Recent ERM Attacks:

Salesforce CRM Compromise via Phishing (August 2025): Attackers, posing as IT staff, tricked employees into installing a malicious application that stole credentials and multi-factor authentication (MFA) codes.

Oracle Cloud Supply Chain Attack (March 2025): Threat actor exfiltrated 6 million records from Oracle Cloud's Single Sign-On (SSO) and LDAP systems by exploiting a potential vulnerability in the *login.oraclecloud.com* domain, which led to unauthorized access to tenant data.

Microsoft Midnight Blizzard Attack (Ongoing from January 2024): Russian SSG Infiltrated Microsoft's corporate email systems. The attackers initially used a password spray attack on a legacy, non-production test tenant account and then leveraged the access to breach corporate email accounts.

Conclusion

Given the hybrid nature of Cloud tech’s environment, continuous risk assessment and mitigation are critical. The outlined plan prioritizes risks that pose the greatest threat to operations and data integrity. Implementing these measures will significantly reduce attack surfaces, improve regulatory compliance, and promote a security-aware organizational culture. Regular monitoring and reassessment will ensure evolving threats are managed proactively.

This report structure aligns with NIST guidelines and best practices for enterprise risk management reports.