T-Mobile Cybersecurity: Scope, goals, and risk assessment report

Scope and goals of the audit

Scope: The scope of this risk assessment encompasses includes T-Mobile's cybersecurity posture, with particular focus on risks associated with network security, data protection, third-party security, and regulatory compliance. This means all assets need to be assessed alongside internal processes and procedures related to the implementation of controls and compliance best practices.

Goals: The goals are to analyze current security controls, identify vulnerabilities, and provide mitigation strategies to strengthen T-Mobile's cybersecurity vulnerability. To do this, evaluate current assets and complete the controls and compliance checklist to determine which controls and compliance best practices are required.

Current assets

- On-Premises & Cloud-Based Security Systems: Firewalls, intrusion detection systems (IDS), and Security Information and Event Management (SIEM) tools.
- Data Protection Mechanisms: Encryption protocols, data retention policies, and multi-factor authentication (MFA).
- Access Management: Privileged access control, role-based access management, and user behavior analytics.
- Network and Endpoint Security: VPNs, anti-malware tools, and endpoint detection and response (EDR) solutions.
- Compliance and Regulatory Frameworks: Policies aligning with GDPR, PCI-DSS, and FCC standards.

Risk description and Monitoring Plan

Risk Name	**Risk Description**	**Monitoring Plan**
Data Breaches	Unauthorized access or exposure of customer data could lead to severe financial and reputational damage.	DLP monitoring, database access tracking, security assessments
Unauthorized Access to Customer Data	Attackers may exploit vulnerabilities to gain unauthorized access to customer records.	Real-time SIEM monitoring, anomaly detection, geo-login alerts
Phishing and Credential Theft	Employees may fall victim to phishing attempts, leading to unauthorized system access.	Email behavior anomaly tracking, unrecognized device flags
Insider Threats	Malicious or negligent insiders could expose sensitive data or compromise security.	User behavior analytics, unauthorized data access alerts
Zero Trust Implementation Challenges	Implementing Zero Trust security may face delays and resistance, creating security gaps.	Security audit tracking, policy adherence monitoring
Third-Party Security Risks	Vendors may introduce security weaknesses through poor security practices.	Vendor cybersecurity score monitoring, SLA enforcement
Regulatory Non-Compliance	Failure to meet compliance requirements may result in penalties and legal actions.	Automated compliance tracking, real-time policy checks

Risk score

On a scale of 1 to 10, the overall risk score is 8, indicating a high-risk level. This high rating is primarily due to:

- A high likelihood of phishing attacks, unauthorized access, and data breaches.
- Increased exposure from third-party security risks and regulatory non-compliance.
- Network and Endpoint Security: VPNs, anti-malware tools, and endpoint detection and response (EDR) solutions.
- Challenges in implementing Zero Trust and insider threat management.

Additional comments

The potential impact from security breaches, unauthorized access, and phishing attack is rated as high, because the complexity of threats and T-Mobile's exposure to financial, operational, and reputational risks. For more specific information, go over the following bullet points:

- Access Controls: Without strict privilege enforcement, employees may be able to access client data.
- Encryption Procedures: Sensitive information and client databases may not fully encrypt.
- Security Operations: Although it lacks automated remedial options, the Security Operations Center (SOC) is capable of monitoring.
- Firewall Protection: While firewalls are in place, rules need to be updated to counter evolving threats.
- Malware Protection: Although antivirus software is in use, threat intelligence streams still need to be enhanced.
- Intrusion Detection System (IDS): Currently lacks comprehensive IDS coverage for cloud environments.
- Incident Response & Backup Strategy: Critical systems require a clear disaster recovery plan.
- Regulatory Compliance: There is inconsistency in the way security rules and compliance assessments are carried out.
- Password Policies: Some password requirements, like demanding multi-factor authentication (MFA).
- Legacy Systems: Security fixes for older systems must be applied manually because they do not have security updates.