T-Mobile Cybersecurity: Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the T-Mobile Cybersecurity Scope, Goals, and Risk Assessment Report. This checklist assesses whether the necessary security controls are in place to mitigate key risks.

Controls assessment checklist

Then, Select “Yes” or “No” to indicate if the control is implemented.

Yes	No	Control
		Least Privilege
		Disaster recovery plans
		Password policies
		Separation of duties
		Firewall
		Intrusion detection system (IDS)
		Backups
		Antivirus &. Malware Protection
		Manual monitoring, maintenance, and intervention for legacy systems
		Data Encryption

		Password management system
		Access Control for sensitive Data
		Security Operations Center (SOC) Monitoring

To complete the compliance checklist, refer to the risk assessment report to ensure T-Mobile adheres to necessary regulatory and security best practices.

Compliance checklist
Then, Then, Select “Yes” or “No” to indicate if the compliance l is implemented.

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
		Only authorized users have access to customers’ credit card information.
		Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
		Implement data encryption procedures to better secure credit card transaction touchpoints and data.
		Secure password manager policies are in place.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
		Always take data protection into account, from the moment you begin developing a product to each time you process data.
		Encrypt, pseudonymize, or anonymize personal data wherever possible.

		Create an internal security policy for your team members and build awareness about data protection.
		Know when to conduct a data protection impact assessment and have a process in place to carry it out.
		Have a process in place to notify the authorities and your data subjects in the event of a data breach.

System and Organizations Controls (SOC type 1, SOC type 2)

Yes	No	Best practice
		User access policies are well-established.
		Sensitive data (PII/SPII) is protected and confidential.
		Data integrity measures ensure accuracy and validation.
		Availability controls ensure authorized access when needed.

Federal Communications Commission (FCC) Compliance

Yes	No	Best practice
		Protect Customer Proprietary Network Information (CPNI).
		Comply with FCC breach notification rules.
		Implement security against telecom fraud & spam prevention.
		Secure telecommunications infrastructure from cyber threats.

National Institute of Standards and Technology (NIST) Cybersecurity Framework

Yes	No	Best practice
		Follow the 5 NIST cybersecurity functions: Identify, Protect, Detect, Respond, Recover.
		Conduct continuous risk assessments.
		Use multi-factor authentication (MFA) and encryption.
		Improve incident response and threat intelligence sharing.

ISO/IEC 27001 Compliance

Yes	No	Best practice
		Implement an Information Security Management System (ISMS).
		Define security policies and conduct risk assessments.
		Perform regular internal and external security audits.
		Ensure continuous monitoring and cybersecurity improvements.

This checklist serves as a foundation for T-Mobile's cybersecurity improvements, helping the organization minimize risk exposure and maintain compliance with regulatory standards.