VioletX x Ramyar Daneshgar

Risk Assessment For XYZ Company

09 11 2025

Executive Summary

Baseline state: Company XYZ is a mid-sized U.S./EU tech firm subject to GDPR and PCI DSS, operating on AWS, GitHub, a remote workforce with local admin rights, and a third-party dev team in Ukraine.

Desired state: Implement a Zero Trust model across infrastructure, source code, and endpoints, meet regulatory compliance and vendor / third party risk management and audit readiness in place.

Agenda

Five current risk vectors

1. Cloud misconfiguration in AWS
2. Source Code Security Weaknesses
3. Endpoint Privilege & Access Control Gaps
4. Regulatory Non Compliance
5. Third-Party & Supply Chain Vulnerabilities

Infrastructure Security Assessment for AWS

IAM Over-Privileging

Excessive IAM roles and policies grant more permissions than needed.

Impact
Increases likelihood of unauthorized access and privilege escalation.

Recommended Action
Enforce least privilege IAM using Access Analyzer, implement role-based access, and require MFA.

Insufficient Audit Logging

Incomplete logging and threat detection coverage, CloudTrail and GuardDuty are not enabled or lack proper retention period.

Impact
Limits forensic visibility and delays MTTD for anomalous activity, privilege misuse, or advanced persistent threats (APTs).

Recommended Action
Enable CloudTrail, GuardDuty, and Security Hub on AWS with centralized log retention (≥12 months). Provision logs to a SIEM/SOAR for unified monitoring, faster threat detection, and automated remediation.

Unprotected Data Assets

Misconfigured S3 buckets and EBS volumes expose sensitive corporate data.

Impact
Leads to risk of data loss, regulatory penalties for noncompliance with GDPR/PCI DSS, and reputational harm / loss of consumer trust.

Recommended Action
Enforce encryption at rest with AWS KMS (automatic key rotation), data in transit with TLS 1.2+/1.3, and apply Block Public Access at the account and bucket level. Continuously monitor storage configurations with AWS Config and Security Hub to detect and remediate misconfigurations.

Flat Network Architecture

Flat network architecture with no segmentation between PCI workloads and general compute.

Impact
Undermines PCI DSS compliance and increases the risk of lateral movement by adversary if the environment is compromised.

Recommended Action
Implement network segmentation with dedicated VPCs, restrictive security groups, and NACLs to isolate workloads.

Source Code Repository Security (GitHub)

Excessive Repository Permissions

Over-privileged developer and service accounts retain read/write access beyond scope of their work.

Impact
Increases likelihood of insider threats, such as account takeover or unauthorized code change / injection.

Recommended Action
Enforce least privilege with role-based access, require SAML SSO + MFA, and mandate signed commits with branch protection rules.

Insufficient Audit Logging

Limited visibility into commit history, pull requests, and access anomalies

Impact
Increases Mean Time to Detection (MTTD) for account compromises, malicious commits / injections, and data loss.

Recommended Action
Enable GitHub audit logs (enterprise), integrate logs events into a SIEM for correlation, and activate GitHub Security Alerts for all repos.

Exposed Secrets & Credential

API keys, tokens, and passwords embedded in source code or configuration files.

Impact
Creates opportunities for credential compromise, unauthorized lateral movement, and software supply chain exploitation through exposed secrets / Intellectual property.

Recommended Action
Use GitHub Advanced Security for automated secret scanning, enforce pre-commit hooks to block sensitive data at commit time, and immediately revoke and rotate any comprised credentials.

Lack of Code Review

Unrestricted / direct pushes and merges to main branches without peer review or controls.

Impact
Enables injection of malicious code into production pipelines.

Recommended Action
Enforce branch protection policies with mandatory pull requests, required status checks, and assign code reviewers.

Endpoint Security Assessment for Remote Workers

Excessive Local Privileges

Endpoints provisioned with persistent local administrator rights.

Impact
Enables privilege escalation, malware persistence, and unauthorized application installs.

Recommended Action
Remove local admin rights, enforce least privilege access with MDM (Intune/Jamf). Use just-in-time elevation with audit logging for approved exceptions.

Inconsistent Patch & Update Management

Devices outside corporate networks miss OS, browser, and application updates.

Impact
Expands attack surface by exposing devices to exploitable CVEs and zero-day vulnerabilities.

Recommended Action
Apply centralized patch enforcement via MDM/Endpoint Manager, automate browser & VPN client updates, and verify compliance with automated vulnerability scans.

Insufficient Endpoint Detection (EDR/XDR)

Remote endpoints lack real-time threat monitoring and advanced detection.

Impact
Reduces visibility into ransomware, phishing payloads, and zero-day threats, delaying incident detection and response.

Recommended Action
Deploy EDR/XDR (Defender for Endpoint), integrate alerts into the SOC/SIEM for centralized monitoring, and implement automated response playbooks.

Weak Remote Access & Authentication Controls

Remote access depends on static credentials without adaptive authentication or data loss prevention (DLP) controls.

Impact
Increases likelihood of data exfiltration, credential compromise, account takeover, compliance violations, and lateral movement if endpoints are lost, stolen, or compromised.

Recommended Action
Enforce full-disk encryption deploy endpoint DLP policies, restrict removable media, and mandate MFA, and Zero Trust Network Access with validation before connectivity is granted.

Compliance Considerations for GDPR & PCI DSS

Shadow IT

Remote workers install unauthorized local apps outside IT authorization.

Impact
Breaches PCI DSS Req. 12.3 (Security Policies for Technology Use) and undermines GDPR Art. 5 (Integrity & Confidentiality).

Recommended Action
Remove local admin rights; enforce least privilege access with MDM (Intune/Jamf). Use just-in-time elevation for exceptions.

Identity Federation & Access Governance Gaps

Fragmented identity management across cloud and on-prem services, with inconsistent policy enforcement.

Impact
Violates PCI DSS Req. 8 (Identify & Authenticate Access) and GDPR Art. 32 (Security of Processing); increases risk of account takeover and inconsistent MFA enforcement.

Recommended Action
Deploy a centralized IAM platform with federated SSO (SAML/OAuth2/OpenID Connect), enforce adaptive MFA across all user groups, and implement continuous, risk-based authentication with session monitoring.

Cross-Border Transfer Risks

Remote endpoints sync sensitive data to cloud storage outside approved regions.

Impact
Non-compliance with GDPR Art. 44–46 (Cross-Border Data Transfers) and PCI DSS Req. 3 (Storage & Protection of CHD); enables unlawful data export.

Recommended Action
Enforce geo-fencing policies, leverage cloud DLP, and mandate data localization controls in endpoint sync/backup configurations to ensure critical data remains within approved jurisdictions.

Insider Threat

Insider threat with exfiltrate sensitive data, while remote endpoints lack tested backup and recovery mechanisms for critical data.

Impact
Violates GDPR Art. 24 (Accountability), GDPR Art. 32 (Availability & Resilience of Processing), and PCI DSS Req. 10 & 12.10.1.

Recommended Action
Implement UEBA for anomaly detection and integrate outputs into SIEM/XDR for correlation and response. Enforce least privilege with granular access monitoring, deploy immutable endpoint backups, and regularly conduct tabletop exercises.

Third-Party Risk Assessment for Ukrainian Dev Team

Cross-Border Data Transfer Risks

Development activities involve access to EU/U.S. regulated data from non-adequate jurisdictions.

Impact
Creates risk of non-compliance with GDPR Art. 44–46 (Cross-Border Transfers), exposing the organization to regulatory sanctions, fines, and invalidation of processing agreements.

Recommended Action
Perform Transfer Impact Assessments (TIAs), enforce data localization and segregation policies, and mandate encrypted VPN tunnels with MFA/SSO for remote sessions.

Vendor Security Maturity

Limited assurance of third-party security controls, governance, and compliance maturity.

Impact
Increases exposure to supply chain compromise, malicious insider activity, and credential-based account takeovers.

Recommended Action
Require SOC 2 / ISO 27001 certification, enforce contractual SLAs for security and breach notification, and conduct periodic third-party security audits and penetration testing to validate controls.

Privileged Access & Identity Governance Risks

Third-party developers maintain persistent or excessive access to code repositories and cloud workloads.

Impact
Facilitates unauthorized code injection, data exfiltration, and lateral movement in the production environment.

Recommended Action
Enforce role-based, least-privilege access with just-in-time elevation, require MFA + federated SSO, and monitor all privileged activity through SIEM/XDR with UEBA correlation.

Software Supply Chain & Code Integrity Risks

Insecure coding practices or compromised development environments may introduce malicious code or vulnerable dependencies.

Impact
Increases risk of dependency confusion, malicious package injection, and downstream regulatory non-compliance.

Recommended Action
Enforce secure SDLC practices, implement branch protection with mandatory peer reviews, and integrate SAST, SCA, and DAST scanning into CI/CD pipelines to detect insecure code and vulnerable libraries before release.

Risk Matrix

Risk	Likelihood	Impact	Overall Rating
AWS misconfigured IAM roles	High	High	**Critical**
Secrets in GitHub repo	Medium	High	High
Local admin on laptops	High	Medium	High
GDPR noncompliance (data transfers)	Medium	High	High
Third-party access risks	Medium	Medium	Medium
Lack of PCI segmentation	Low	High	**Medium**

Next steps

Step 1

Critical (Immediate Attention – 0–30 Days)
Lock down AWS IAM (least privilege + MFA), remove local admin rights, and enforce AWS encryption (KMS + TLS 1.2/1.3).

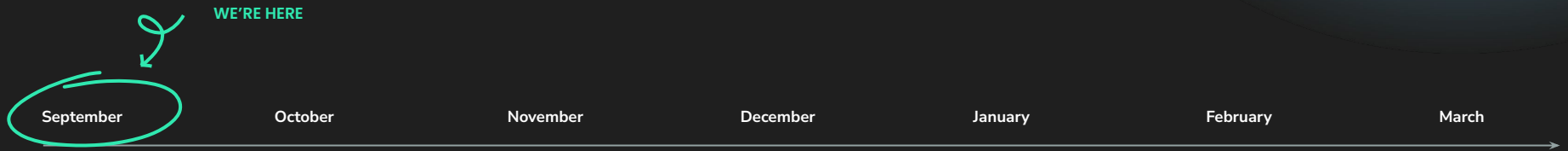
Step 2

High (30–90 Days)
Secure GitHub repos (SSO/MFA, branch protection, secret scanning), embed SAST/DAST/SCA in CI/CD, and deploy EDR/XDR with SIEM integration.

Step 3

Medium (90-180 days)
Audit Ukrainian vendor security, implement PCI DSS-compliant network segmentation, and enable continuous compliance monitoring with UEBA.

Remediation Timeline



(Sep 11 – Oct 12, 2025)

Step 1 - Critical

This phase focuses on closing the most urgent attack vectors. AWS IAM roles are locked down with least privilege and MFA, centralized logging is enabled for audit readiness, and all AWS data is encrypted. On endpoints, persistent local admin rights are removed to prevent privilege escalation and malware persistence.

(Oct 13 – Dec 12, 2025)

Step 2 - High

GitHub repositories are secured with SSO/MFA, branch protection, and secret scanning. Security testing (SAST/DAST/SCA) is embedded directly into CI/CD pipelines to prevent vulnerable code from reaching production. GDPR Transfer Impact Assessments are completed to ensure lawful cross-border processing, while EDR/XDR is deployed for advanced endpoint detection with SIEM integration.

(Dec 13, 2025 – Mar 12, 2026)

Step 3 - Medium

The focus expands to long-term resilience and vendor assurance. A full security audit of the Ukrainian development team is conducted, ensuring SOC 2 / ISO 27001 alignment. AWS networks are redesigned for PCI DSS-compliant segmentation to isolate sensitive workloads. Continuous compliance monitoring is deployed across AWS, and UEBA capabilities are introduced to detect insider threats and anomalous account behavior.

Works Cited

Amazon Web Services. AWS Security Best Practices. AWS Whitepaper, Amazon Web Services, Inc., July 2023, https://docs.aws.amazon.com/whitepapers/latest/aws-security-best-practices/aws-security-best-practices.pdf

European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). Official Journal of the European Union, L119, 4 May 2016, pp. 1–88.

PCI Security Standards Council. Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures, Version 4.0. PCI Security Standards Council, Mar. 2022.

Thank you!

ramyarda@usc.edu