

Core RiGoR Review

Q1'25 Cybersecurity Update

January 27, 2025 | Core Risk Governance Review program

Heather Adkins, VP Security Engineering

Ex. No.
PXR0302

1:20-cv-03010-APM

1:20-cv-03715-APM

GOOG-DOJ-34940297

Top Cybersecurity Risks | Overview

Insider Risks

Intellectual Property (IP)

Very High Risk. • On Track Insider access to Intellectual Property including Al Models.

User Data Protection

Very High Risk On Track Insider access to user data in storage repositories.

Access Controls in First-Party Tools (1P)

High Risk.

On Track

Insider access to user data via 1P Enterprise Tools.

Third-Party Risks

Third-Party SaaS (3P)

High Risk.

On Track

Use of third-party Software as a Service solutions.

Contract Manufacturing (CM)

High Risk.

On Track

Third-party Contract Manufacturing facilities that make Google's servers and consumer devices.

Software Supply Chain

High Risk.

On Track

Software creation, maintenance, and deployment.

Trusted Identity Risk

Identity Verification & Deepfakes (IdV)

Very High Risk. • On Track

Threat actors impersonating employees and members of the extended workforce.

Infrastructure Risks

Physical Infrastructure Controls **Systems**

Very High Risk

On Track

Physical Infrastructure Controls Systems that manage water, power, cooling, etc., in data centers.

Developer Endpoints

High Risk.

On Track

Highly-privileged engineering workflows.

Alphabet's Use of Cloud

High Risk

Off Track

Use of next-gen Cloud platforms.

Data Center Regionalization

High Risk

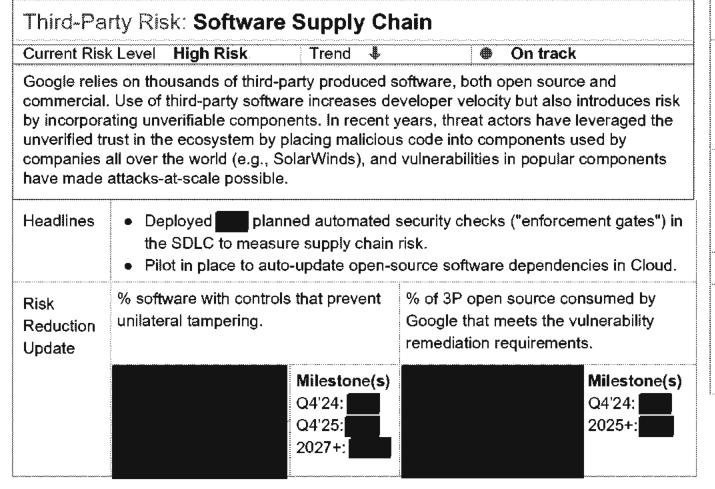
On Track

Expanded data center locations and services.

Confidential and Proprietery 6

Office of Cybersecurity Resilience

HIGHLY CONFIDENTIAL GOOG-DOJ-34940304



Additional Context

Google has historically mandated code tampering controls, such as requiring two-person review on all code. Our work on additional controls will continue to drive down risk.

2026 Risk Target

Medium Risk

Our focus is on updated automation, control development, and increased control adoption, with broad take-up in 2026.

Control Maturity

Ad Hoc

We have not yet developed all the solutions we need to scale control enforcement. We may not have a complete inventory of assets to be protected.



🦃 Cifice of Cybersecurity Resilience

Confidential and Prosingery 22

HIGHLY CONFIDENTIAL

GOOG-DOJ-34940327

Third-Party Risk | Software Supply Chain

Overview

Third-party dependency management is fundamental to Google's software supply chain. We have obligations to Google and our Customers to protect and be transparent about our software supply chain.

Challenge(s)

- Shared fate: The Core-administered third-party google3 directory is shared across Google.
- Federated ownership of shared third-party dependencies in google3 does not scale. Central remediation continues to have the largest ROI on safety and security.

Path forward

Pursuant to the Core Pillar Request and Internal Audit findings.

- 1. Automation: Build infrastructure to automate maintenance of dependencies.
- 2. Pay down accumulated risk debt: Remediation of select dependencies and moving them onto well-lit paths with automated maintenance. Prioritize Trusted Core Access (TCA) C++ dependencies going forward.

📢 - Core Pillar Request

Support for Beyond Security funding to relevant Core teams (Core Dev, PSS) and TRR (in progress).

🕠 Office of Cybersecurity Resilience

Confidential and Proprietery 23

HIGHLY CONFIDENTIAL GOOG-DOJ-34940328