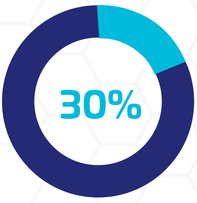
Third-party identities: your hidden compliance risk

Third-party identities are essential - but they're also a growing risk. Failing to act can lead to fines, business disruption, or worse.



of data breaches in 2025 are linked to third-party access - twice as many as 2024[1]

$4.81M USD

the average cost of a third-party breach, about **$250,000** more than internal incidents[2]

CSP (NIST Cybersecurity Framework) Must assess and manage third-party cyber risk

HIPAA (Health Insurance Portability and Accountability Act) Requires Business Associate Agreements (BAAs) with vendors handling Protected Health Information (PHI), plus access controls.

CMMC (Cybersecurity Maturity Model Certification) Defense contractors need identity proofing, MFA, auditability

GDPR (General Data Protection Regulation) Requires third-party service providers ("processors") to show they have proper data protection controls in place.

NIS2 (Network and Information Security Directive 2) Requires organization to secure their supply chain, including third-party access and systems.

DORA (Digital Operational Resilience Act) Requires centralized identity management and controls to monitor third-party risk.

National Strategy for Critical Infrastructure Third parties must ensure adequate data protection

Privacy Act & PIPEDA Organizations remain accountable for data shared with vendors and processors

CPS 230 (Cross-industry Prudential Standard on Operational Risk Management) Requires banks, insurers, and super funds to identify, assess, and manage operational risks from material service providers — including cybersecurity and access controls

Common themes across jurisdictions:

- **Data minimization:** Only collect identity attributes necessary for access and use.
- **Contractual controls:** Data processing agreements with third parties are often mandatory.
- **Auditability:** Must maintain records of access and data processing activities.
- **User rights:** Third-party users may have the right to access, correct, or delete their data.
- **Security and accountability:** Must provide strong access controls, encryption, and monitoring capabilities.

Third-party access compliance is no longer optional

- **DORA effective from January 2025. Financial entities must already have third-party oversight programs in place.**
- **CPS 230 effective July 2025. APRA expects proactive compliance and testing ahead of the date.**
- **CMMC falling out in FY2025. Contracts a lready require evidence of compliance readiness.**

How can Thales Help

Thales helps organizations enforce access controls and comply with a wide range of regulations, wherever they operate.

[1] Verizon's 2025 Data Breach Investigations Report
[2] IBM/Ponemon, 2024 Cost of a Data Breach Report