Outsourced development

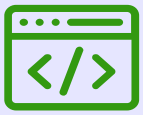
ISO 27002 Control 8.30

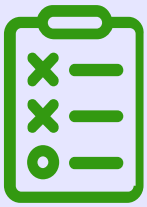
Control

The organization should direct, monitor and review the activities related to outsourced system development

Purpose

To ensure information security measures required by the organization are implemented in outsourced system development



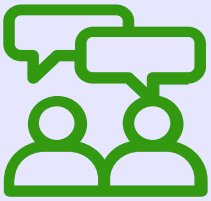


Why is it important?

- The organization maintains responsibility for the security of its systems, even if developed externally
- Contractual terms are necessary to enforce the organization's secure development standards
- Mitigates risks related to intellectual property ownership and supplier failure (escrow agreement)

What could we do ?

- Third-party risk assessment and due diligence
- Secure code escrow agreements
- Non-disclosure agreements (NDAs)
- IP and data ownership contracts
- Vendor security audits and certifications
- Code review and quality gates
- Restricted access to production environments
- Background checks for contractors
- Secure communication channels (VPNs, encrypted)
- Supply chain security and SBOM requirements



Details

- Requirements should cover the security of the supplier's development environment
- The supplier should be provided with the threat model to consider
- Assurance reports (e.g., third-party attestations) can provide evidence of supplier security capabilities
- Compliance with personal data protection legislation must be considered

Link with other frameworks

- NIST 800-53 rev5 : SA-4, SA-10, SA-11, SA-15, SR-2, SR-4
- NIST CSF 2.0 : DE.CM-06

Renaud Dardenne
Asphalia Consulting