

External Security Audit

External Security Audit

The External Security Audit is a key process managed by the SIP (Security, Integrity, and Protection) Office at Syensqo. Its main goal is to assess and validate the security posture of IT solutions and third-party vendors before deployment or contract signature.

Purpose:

- Identify and manage risks related to IT solutions and external partners.
- Ensure compliance with Syensqo's internal policies and regulatory requirements.
- Provide assurance that security controls are in place and effective.

How It Works:

1. **Initiation:** The process begins when a project team or stakeholder contacts the SIP Office to request an audit.
2. **Information Gathering:** The team and vendor complete risk and cybersecurity questionnaires, providing necessary documentation.
3. **Analysis:** SIP analysts review the information, conduct technical assessments (such as penetration tests or configuration reviews), and may request clarifications.
4. **Reporting:** The SIP Office delivers a summary report, including a security annex for contracts or a residual risk report for solutions, with clear recommendations.

Key Deliverables:

- Security annex for vendor contracts
- Residual Risk Restitution report for IT solutions
- Cybersecurity Requirements Exhibit (CSRE) for vendors

Integration: The audit process is embedded in Syensqo's project and procurement workflows, ensuring that security is considered from the earliest stages of any new initiative or contract renewal.

Contact:

For more information or to initiate an external security audit, reach out to the SIP Office at sip-office@syensqo.com.