

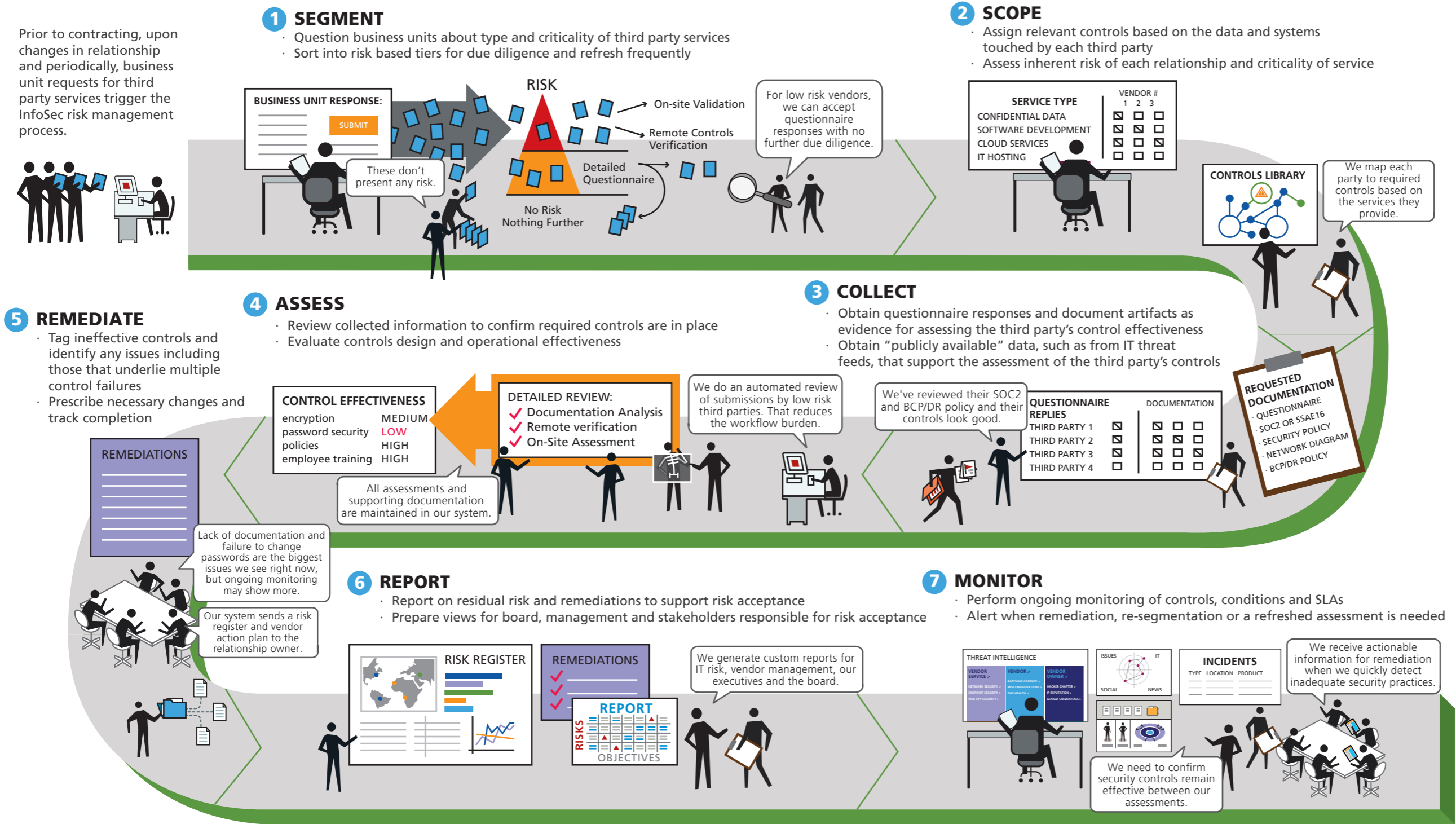
Managing Third Party InfoSec Risk

Cyber attacks cost businesses more than \$400 billion in 2015. Since two thirds of those attacks were perpetrated on and through third parties handling company or customer data, it's vital that information security be applied across the extended business enterprise. Managing the process of verifying, remediating where necessary and monitoring the effectiveness of third party controls demands the use of sophisticated and mission-designed technology. In this illustration, we define the key steps of the process and identify what the future holds for third party information security management.

DEVELOPED BY



WITH CONTRIBUTIONS FROM



HOW TECHNOLOGY HELPS:

- Segment**
- Simplify and accelerate collection of data from business
 - Assess for materiality and criticality
 - Automate workflows and approvals of no risk vendors
- Scope**
- Map controls to third party functions
 - Link third party touch points through common taxonomy
 - Flag needed updates based on changed factors
- Collect**
- Streamline collection of questionnaire responses and supporting documents
 - Ensure evidence required for control assessment is readily available
 - Correlate publicly available vendor system security data with controls
- Assess**
- Automate creation of assessment workpapers
 - Store detailed audit results in an actionable, reportable database
 - Leverage templates and content to meet best practices
- Remediate**
- Focus on ineffective controls
 - Support negotiation of remediations and track status
 - Facilitate well-documented, efficient communications
- Report**
- Facilitate real-time visibility
 - Replace separate spreadsheets with actionable data
 - Use calculated risk model to enable consistent risk ratings
- Monitor**
- Collect security system data and metrics for critical vendor performance
 - Correlate system security and threat data to risk controls
 - Manage risky third parties through automated alerts

TIPS FOR DOING IT RIGHT

- Use cloud-based system or SaaS solution to centralize documentation and work flows between internal and third party users.
- Involve multiple stakeholders across the organization in identifying relevant control frameworks and risk level attributes.
- Define standard contract clauses for data protection, privacy, fourth party controls, remediation of issues and end of relationship needs.
- Design audience specific dashboards and reports using advanced data analytics to communicate to the board and management.
- Consider supplementing your program with assessment consortiums and threat intelligence providers.