Managing Third-Party InfoSec Risk

By some reports, cyber-attacks cost businesses $400 billion in 2015 and will exceed $6 trillion annually by 2021. A majority of attacks were perpetrated on and through third parties. Managing the process of verifying, monitoring, and ensuring the effectiveness of third-party controls demands the use of sophisticated and purpose-built technology. In this Illustration, we define the key steps of the process and identify what the future of technology holds for third-party information security management.

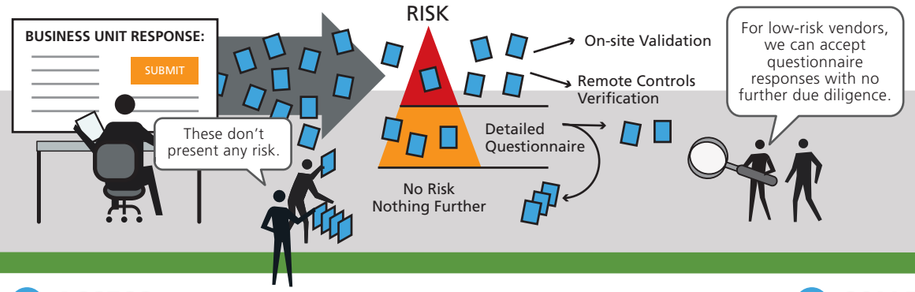
DEVELOPED BY OCEG

WITH CONTRIBUTIONS FROM hiperos Grant Thornton Logic Manager™

Business unit requests for third-party services, changes in the relationship, and scheduled reviews trigger the InfoSec risk management process.

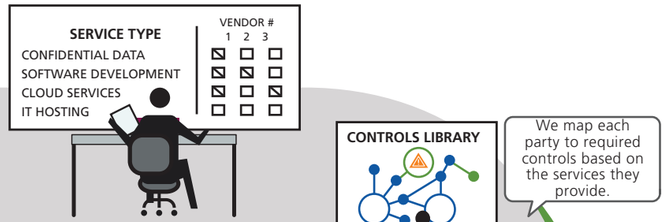
1 SEGMENT

- Question business units about type and criticality of third-party services
- Sort into risk-based tiers for due diligence and refresh frequently



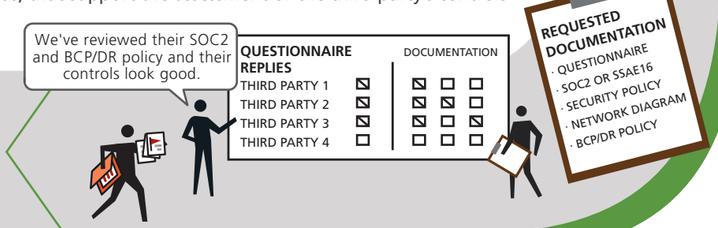
2 SCOPE

- Assign relevant controls based on the data and systems touched by each third party
- Assess inherent risk of each relationship and criticality of service



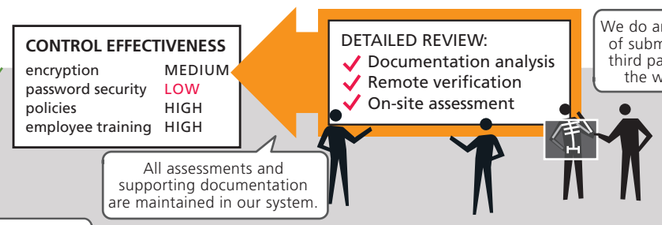
3 COLLECT

- Obtain questionnaire responses and document artifacts as evidence for assessing the third party's control effectiveness
- Obtain "publicly available" data, such as from IT threat feeds, that support the assessment of the third party's controls



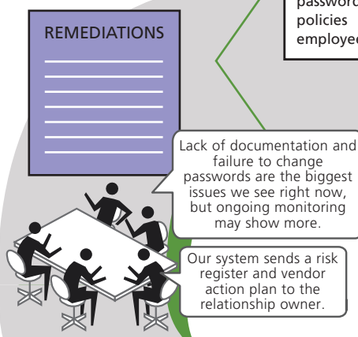
4 ASSESS

- Review collected information to confirm required controls are in place
- Evaluate controls design and operational effectiveness



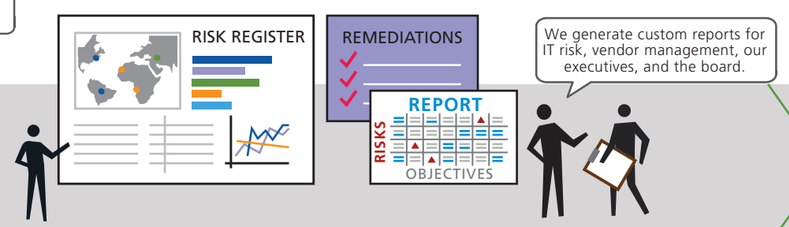
5 REMEDIATE

- Tag ineffective controls and identify any issues including those that underlie multiple control failures
- Prescribe necessary changes and track completion



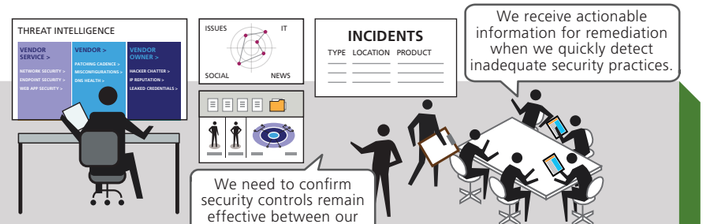
6 REPORT

- Report on residual risk and remediations to support risk acceptance
- Prepare views for board, management, and stakeholders responsible for risk acceptance



7 MONITOR

- Perform ongoing monitoring of controls, conditions, and SLAs
- Alert when remediation, re-segmentation, or a refreshed assessment is needed



TIPS FOR DOING IT RIGHT

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

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