Vendor Risk Management

Castle leverages and relies upon the security of its vendors in order to protect both its own and customer information. Because of this, Castle regularly reviews the security posture of all of its critical vendors and suppliers. Although vendor oversight is the primary responsibility of the finance department, the vendor risk review is a joint activity of the finance and information security teams.

A risk-based approach is taken for vendor security oversight, where more rigor and in-depth analysis is applied to vendors with whom sensitive data is exchanged, or who have the ability to significantly degrade platform availability. Current there are three vendor risk tiers:

- **Tier 1 (High)**: Vendors that directly receive customer sensitive data; vendors necessary for operation of the Castle service platform.
- **Tier 2 (Medium)**: Vendors that do not receive customer-owned data, and are not directly responsible for delivering the service platform. However, disruption in these vendors could significantly degrade Castle's ability to monitor or manage the platform.
- **Tier 3 (General)**: All other vendors.

All vendors are subject to annual review of security, but different focus and scrutiny are directed to different vendor tiers, as follows:

Review Area	Tier 1	Tier 2	Tier 3
Compliance Status	X	X	X
Compliance Report Details	X		
Contractual Confidentiality Terms	X	X	X
Data Retention	X	X	
Data Security Controls	X		
Disaster Recovery / Business Continuity	X	X	
Risk Level Categorization	X	X	X

Review Criteria

Below is a list of sample criteria for review for each of the areas above:

- **Compliance Status**: What compliance standards does the vendor adhere to? When was the last internal/external compliance audit?
- **Compliance Report Details**: Review the most recent compliance report(s) to evaluate specific security controls that are relevant to the service. Ensure that such controls meet or exceed appropriate Castle requirements.

- **Contractual Confidentiality Terms**: Verify that the master service agreement or terms of service include specific confidentiality terms and protection of any data Castle will share with the vendor.
- **Data Retention**: Review what the vendor's data retention periods are, and for any sensitive data, if they define data removal timelines and/or procedures.
- **Data Security Controls**: Review the specific technical and process controls in place for protection of any sensitive data that Castle might share with the vendor.
- **Disaster Recovery / Business Continuity**: Review the vendor's readiness for large scale disruptions of service, uptime objectives, SLAs, and response times to ensure that the service fits within any relevant Castle internal or external SLA targets.
- **Risk Level Categorization**: Verify that the risk tier in which the vendor is sorted (e.g. Tier 1, 2, or 3) is still appropriate to the way in which the vendor's services are being leveraged by Castle.

New Vendors

Prior to engaging any new vendors or suppliers, their security must be reviewed in accordance with this policy. Once the vendor has been categorized based on the nature of the service, review of the vendor's security relative to the corresponding risk tier, is to be done prior to sharing any Castle or customer data with the vendor.