1.1 Security Program Governance

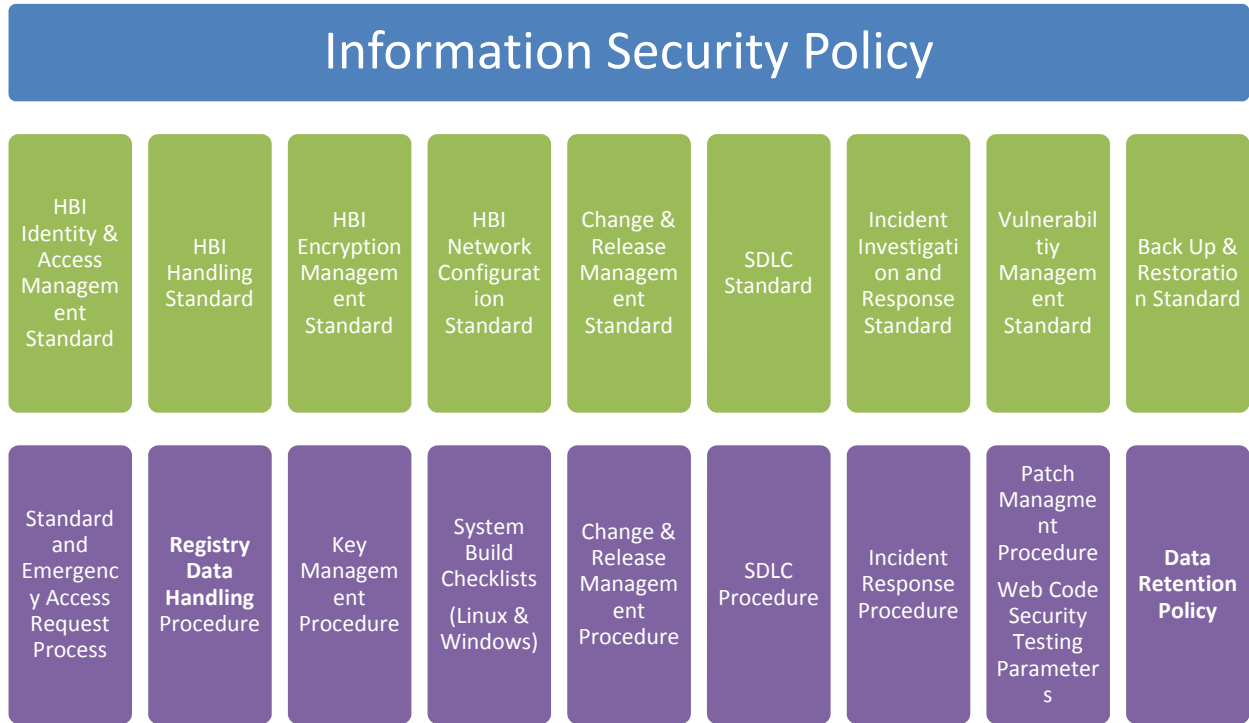| Information Security Policy |
|:---:|

HBI Identity & Access Management Standard	HBI Handling Standard	HBI Encryption Management Standard	HBI Network Configuration Standard	Change & Release Management Standard	SDLC Standard	Incident Investigation and Response Standard	Vulnerabiltiy Management Standard	Back Up & Restoration Standard
Standard and Emergency Access Request Process	**Registry Data Handling** Procedure	Key Management Procedure	System Build Checklists (Linux & Windows)	Change & Release Management Procedure	SDLC Procedure	Incident Response Procedure	Patch Managment Procedure Web Code Security Testing Parameters	**Data Retention Policy**

Figure 1 – Enterprise Risk Oversight

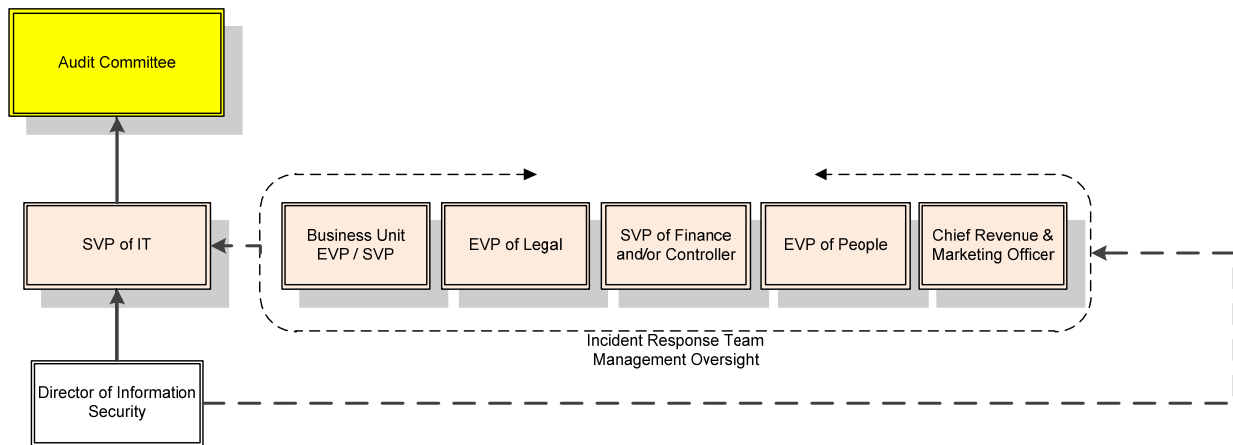## 4.0 Executive Oversight of Business and Security Risks

Figure 2 – Enterprise Risk Oversight

4.1 eGRC: RSA Archer

ENTERPRISE MANAGER

The Enterprise Manager is the central control of all GRC modules correlating the relationships of systems, data and business ownership, asset classification, dependencies within the enterprise hierarchy, compliance requirements, etc.
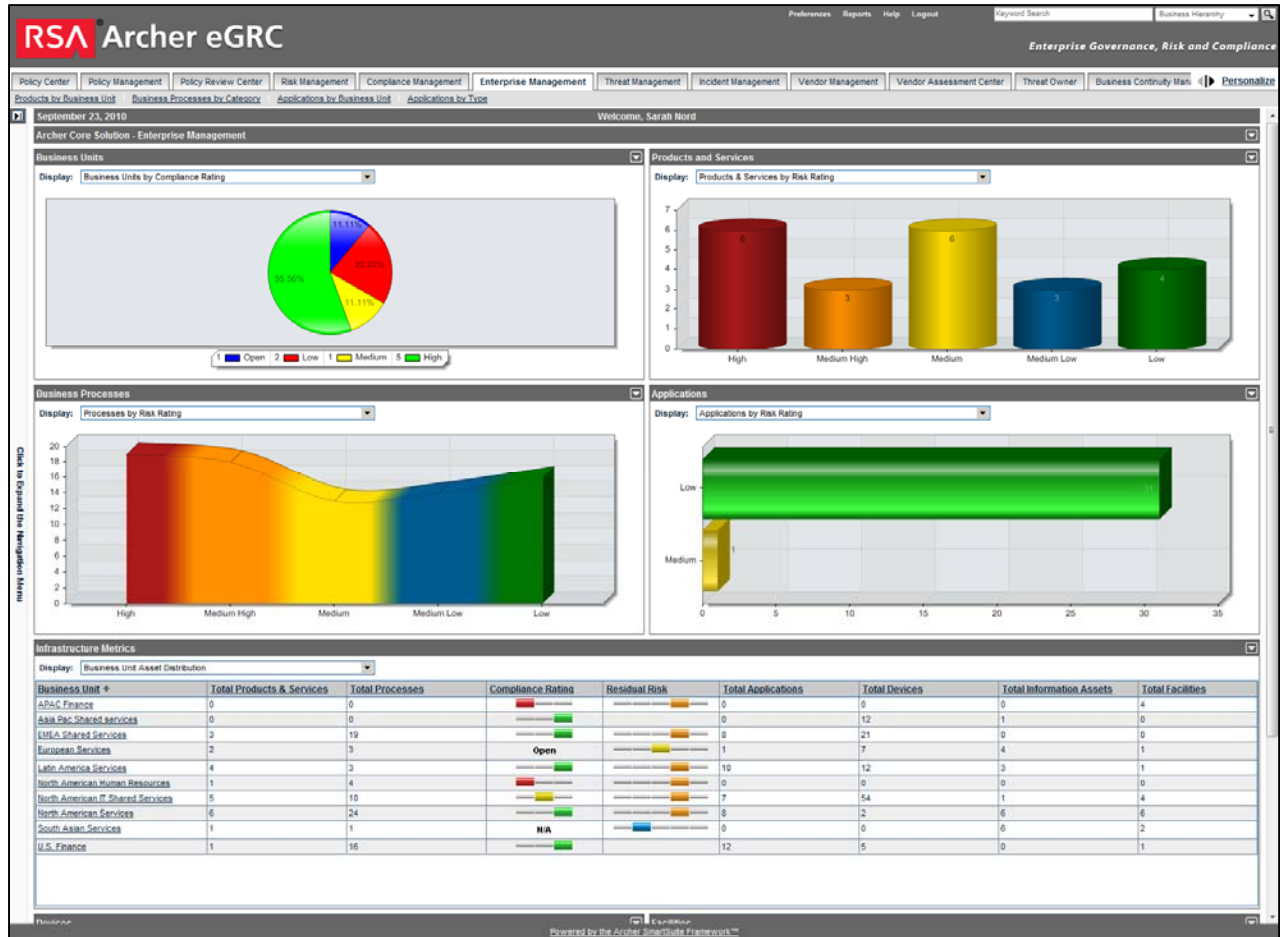

Figure 3 – RSA Archer Enterprise Management Dashboard (sample screenshot - not actual)

POLICY MANAGER

The Policy Management component correlates all of our compliance requirements to control requirements within the Security Policy and Standards in which to automate compliance reporting and employee compliance. (This Policy Manager module will replace the existing "Policy Portal" in April of 2012.)

Figure 4 – RSA Archer Policy Management Dashboard (sample screenshot - not actual)

COMPLIANCE MANAGEMENT

The compliance management solution automates the compliance control testing processes and self-assessments, through test plan execution and integration with third-party scanning tools that continuously monitor compliance with the technical controls and reports on compliance status at the control, business unit and system level.
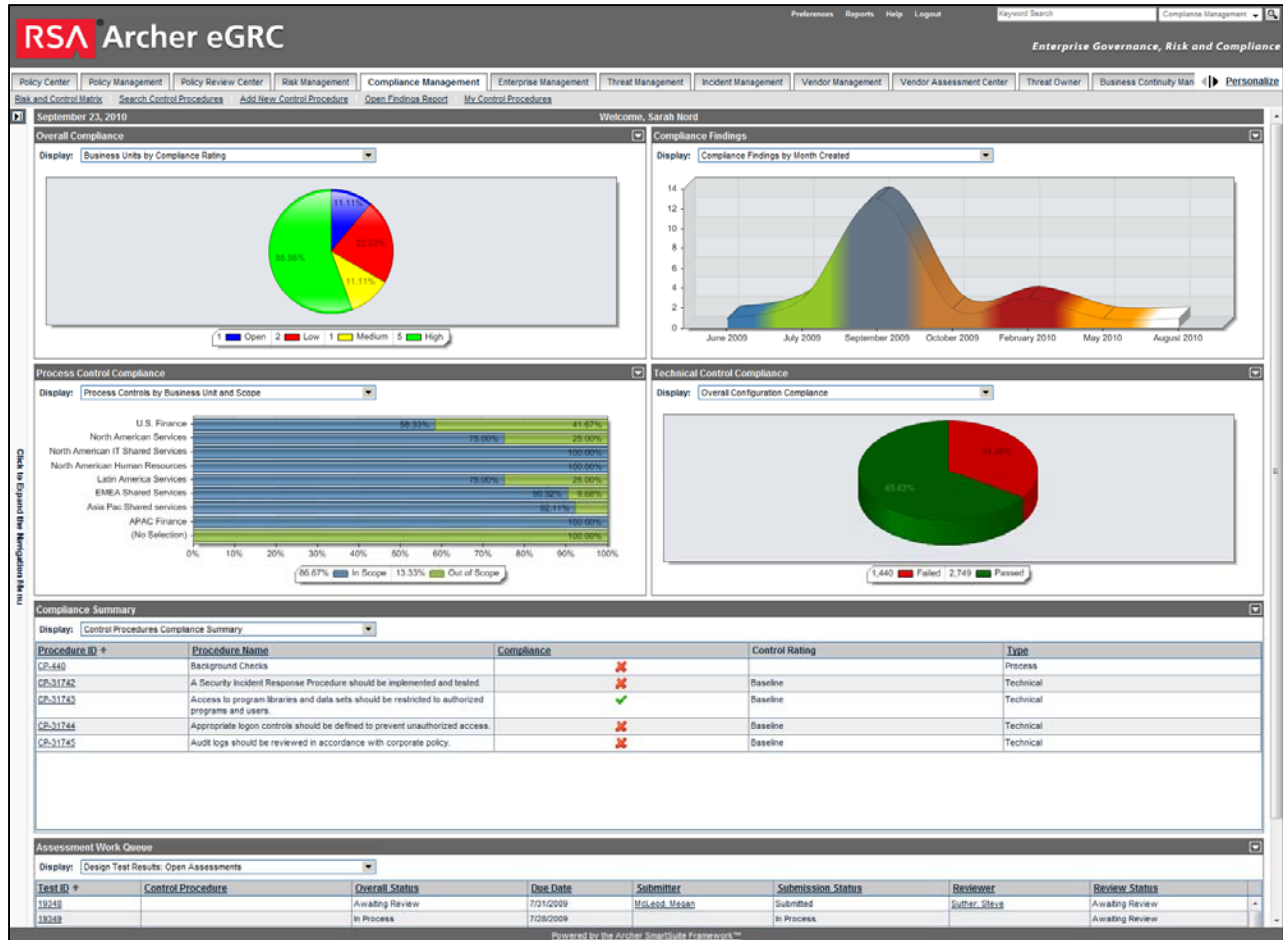

Figure 5 – RSA Archer Compliance Management Dashboard (sample screenshot - not actual)

THREAT MANAGER

The Threat Management module automatically consumes threat feeds from many third party sources such as Microsoft or CERT and our internal vulnerability scanning systems such as Whitehat and Nexpose, and IDS solutions to automate threat reporting per system and automatically alert the system owner.
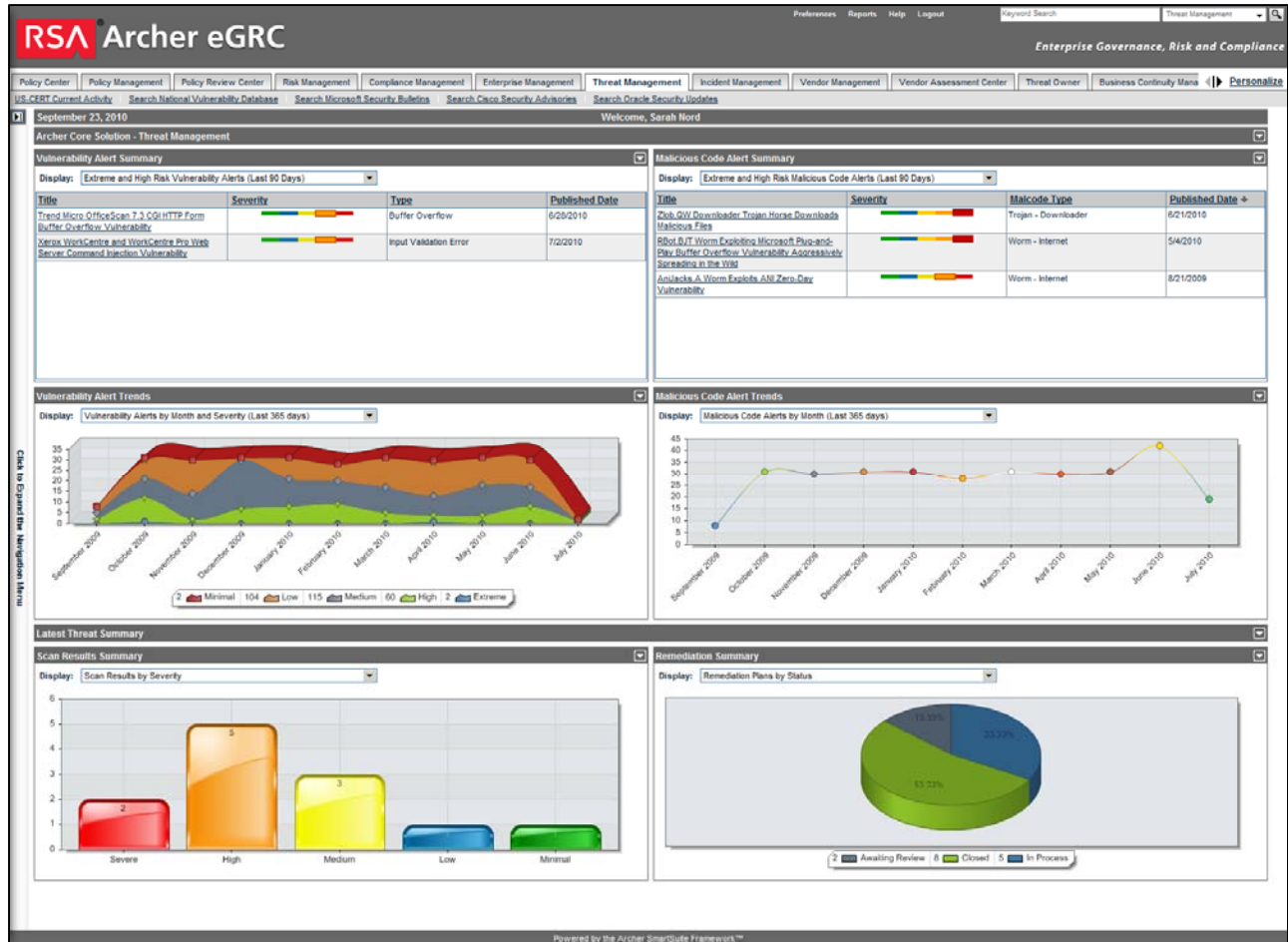

Figure 6 – RSA Archer Threat Management Dashboard (sample screenshot - not actual)

RISK MANAGEMENT

The Risk Management component correlates all the threats identified per system and compliance status and automatically calculates risk scores. Risk scores are evaluated at the Enterprise level or by business unit, and at the individual system level or data classification type. This module maintains a repository of qualitative, quantitative and trending metrics, associates financial metrics to risk, and assists in qualifying the organizations inherent and residual risk through real-time reporting.
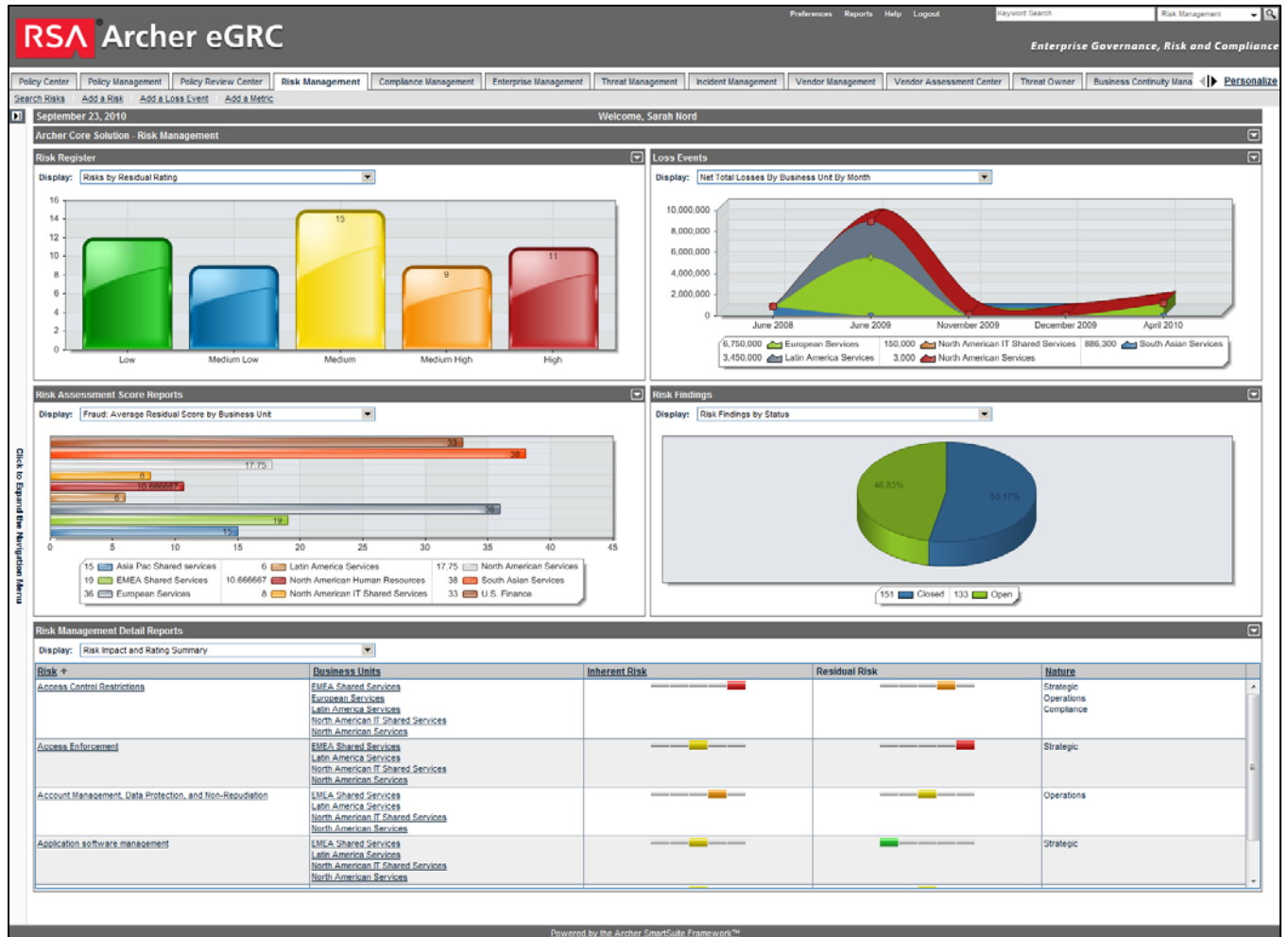

Figure 7 – RSA Archer Risk Management Dashboard (sample screenshot - not actual)