

Software Assurance Forum

Software Security and Implications on Architecture and Vendor Management

Elliott Glazer, MaxSecurity LLC

12 March, 2010

Application Security

Development Policies, Guidelines and Reference Architectures

Requirements Phase

Risk Assessment
Security Requirements Analysis
COTS SDLC Processes
FISAP Shared Assessment

Design Phase

Security Design Review
Security Reference Architecture

Build Phase

Static Analysis
Code Reviews for Security

Test Phase

Dynamic Analysis
OWASP Test Plan
End to End Security Assessment
Database Security Assessment

Operational Phase

Application Logging
Database Information

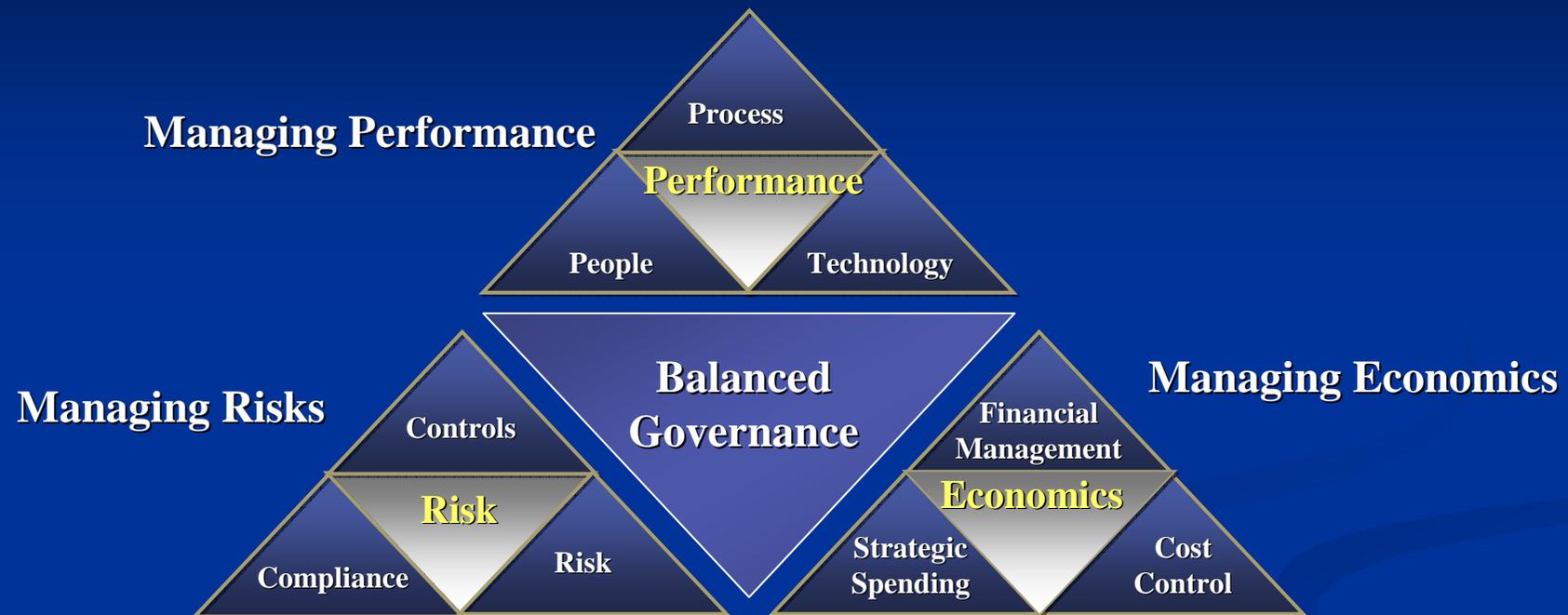
Governance

KPIs and Accountability Reporting

Security Education

Maven Program, Developer, Tester, Leadership

Governance Principles



- Software security is about code you build, code you buy and services you procure
- Using a Risk Based approach to security is needed to make an efficient program
- Vendors should be required to demonstrate the same level of controls as required internally
- Security Architecture is essential to getting software security to work effectively, as it provides the company framework used to build or buy products
- Self Servicing capabilities significantly aids the adoption of controls and improves effectiveness of the program

Vendor Management Processes

- **A full program includes many processes. Some of these are:**
 - **Risk Process for Vendors**
 - Use to determine security requirements
 - Need a set of criteria to evaluate and establish risk
 - **Software Process for COTS and Service providers**
 - Artifacts for their secure development process
 - Code Analysis and standard process
 - FISAP to evaluate services
 - Web Services and Federated Identity
 - **Accountability Model and Process – the Vendor Rating System**
 - **Tracking Non-Compliance and Escalation Processes**
 - **Contract Management Processes**
 - RFP / RFI
 - Standard Security Section for all Contracts based on Risk
 - Standard SLA

Security Architecture Life Cycle

Function	Sub Function	R+D	Pre Invest	Invest	Maintain	DisInvest	Exit
This is the same overlay as all the other Technical Architecture views and comes directly from the Functional Architecture	This is the same overlay as all the other Technical Architecture views and comes directly from the Functional Architecture.	This category is filled with products that should be in a Tech Evaluation Process. This category generally leads to products moving to INVEST, and drives the overall uplift process of solutions. Products determined to be ready for INVEST must be aligned with Development and Operational groups in terms of their readiness to absorb	Products in this category have been determined appropriate for company usage, and are being readied by Development and Operational groups for rollout and productization. Education, training, security configurations, establishment of any controls and governance needs occur during this time period. Generally products will be in this category for 3 months, to complete this cycle, but it will vary based on the complexity of the rollout. Project Plans may be required to complete such rollouts, and at a minimum, a checklist is reviewed to ensure all items have been completed, which includes at a minimum, the above	These solutions are the core solution for the enterprise. Items found in this category are meant to be the standard solutions for the enterprise. If there is no solution that matches the functional needs in this category, look to the Maintain category for the solution	These products continue to meet the needs of the enterprise, and may continue to be used. Products in this space however, may soon be replaced by other solutions, so users should be aware these may change soon, which means they may move to DISINVEST. The decision to move to DISINVEST will be made with senior leadership such as the CISO and CIO or a Security Committee. Solutions in Invest have priority and should be used as the primary solution, before using these solutions. If a service or application is already using these Maintain solutions, it is not intended to drive migration to any INVEST solution however. Maintain solutions are good, valuable solutions, worthy of continued investment. Convergence and simplification strategies however, may show that INVEST solutions will take preference over these, over time	These products have been determined not to be effective anymore and should be replaced. A product in this space should be migrated from within 18 – 24 months of first being determined in this space. All users and usage should be migrated within this time. Security standards must be updated during this time to reflect any changes also. After this time expires, a decision will be made to push these solutions into EXIT by senior leadership such as the CISO and CIO or a Security Committee. Exceptions are required to expand or continue to invest in these solutions, as migration should be occurring, not additional spend on these solutions	These products are out of compliance. No exceptions are allowed for them. They should be gone already. They create significant security risks if they remain. Any such products or groups using such products are reported to both senior leadership and Audit

Accountability Model

Domain	Supply Chain Mgmt (Offshore Controls)	Operations Support (SCAP Support)	Configuration Management (Secure Defaults Shipped or Supported)	Secure SDLC Process (Binary Static Results)	Risk Score
Vendor 1	Green	Green	Green	Green	Red
Vendor 2	Green	Green	Red	Green	Red
Vendor 3	Green	Green	Green	Green	Green
Aggregate	Green	Green	Red	Green	Yellow
Business 1	Green	Red	Green	Green	Yellow
Business 2	Green	Green	Green	Green	Yellow
Aggregate	Green	Red	Yellow	Green	Red

FSSCC Activities

- FSSCC-FBIIC Cyber Security Committee Supply Chain Working Group Toolkit - Hardware Testing
<http://www.fsisac.com/files/public/db/p188.pdf>
- FSSCC-FBIIC Cyber Security Committee Supply Chain Working Group Toolkit - COTS Software
<http://www.fsisac.com/files/public/db/p187.pdf>
- FSSCC-FBIIC Cyber Security Committee Supply Chain Working Group Toolkit - Services
<http://www.fsisac.com/files/public/db/p186.pdf>
- FSSCC-FBIIC Cyber Security Committee Supply Chain Working Group Toolkit - Internal Software Development
<http://www.fsisac.com/files/public/db/p185.pdf>

Thank You

Ajoy Kumar

Depository Trust and Clearing Corp

212-855-7552

AKumar@DTCC.com

Elliott Glazer

MaxSecurity LLC

804-475-5860

ElGlazer@MaxSecurityLLC.com