Integrated Security Architectural Framework

Integrated IT Security Framework

Google "integrated security frameworks" and you'll get a mixture of implementation guidance on specific areas such as authentication, web, or network services. You might also find information on general business practices and governance. Something security practitioners are also looking for is a way to integrate an organization's security efforts with its business needs. They need a means of communicating how their security efforts effectively support the business mission.

The Cisco Global Government Solutions Group implements an integrated IT security framework that ties business processes to risk while identifying gaps in regulatory standards, industry standards, and security policy compliance. This framework provides decision makers with information that can be referenced to help prioritize projects while addressing security in a cost-effective manner. The framework additionally supports organizational survivability following a disaster by directly feeding quantitative risk data into business continuity management.

Business owners can quickly see the end-to-end relationships between the framework's elements. Security practitioners can quickly show the risk addressed by each element and can measure each IT security service's delivery across the framework.

Industry Best Practices

Industry standards in information assurance exist in various areas, including the financial and healthcare industries and public and private sectors. Adherence to one or more of these standards may fulfill specific regulatory requirements but may leave gaps in critical information assurance areas. In other words, one standard may address data integrity and availability but ignore data confidentiality altogether. Adherence to some standards leaves gaps in information assurance even as those standards guide compliance to their own set of requirements.

If security practitioners align to more comprehensive codes of security practices, will they be able to clearly illustrate compliance to the other standards? For example, if security practitioners align to International Organization for Standardization 2700x (ISO), can they still show compliance to Sarbanes-Oxley (SOX), The Committee of Sponsoring Organizations of the Treadway Commission (COSO), The Control Objectives for Information and related Technology COBIT, or Health Insurance Portability and Accountability Act (HIPAA)? What if an organization supports both public and private sector customers? Can it additionally show compliance to NIST-SP800 series, FISMA, NISPOM, or DCID-6-3? Not without a comprehensive information security framework. While you can find crosswalk tools that map the various requirements from NIST to COSO to ISO to HIPAA, etc., these tools do not map back to the organization's projects, programs, and security services.

Framework Adaptability

"Bolting" security controls onto existing IT and business infrastructures is a common undertaking for many organizations, with varying degrees of success. As business needs change, the security framework needs to be robust enough to support the organization's evolution while maintaining comprehensive yet cost-effective protection of the organization's assets.

Consider questions such as:

- Is the organization secure enough?
- How effective are our controls?
- Will the business survive a disaster?

Neither high-level frameworks nor point solutions alone can solve these challenges. What is needed is a means to bridge the high- and low-level strategies such that business processes are tied to risk. The high-level vision provides comprehensive coverage that translates into more effective lower-level solution implementations. This type of end-to-end framework provides a foundation that decision makers can reference during control selection, project prioritization, and business plan creation.

This paper presents a robust security framework that takes an enterprise view of security policy, risk, compliance, and business continuity management down to the business program level and then quantitatively measures service delivery, risk, and compliance.

Industry Approach Challenges

First, let's take a quick look at a few challenges to implementing policy, risk, compliance, and business continuity management in isolated management efforts.

- Isolated policy management can produce granular policies that are often technology-specific. These policies can be difficult to enforce across multinational organizations, resulting in wholesale policy exceptions or conflicting regional requirements. This is most apparent following a merger or acquisition in which the corporate policies are so specific that the acquired organization simply cannot comply within its existing infrastructure.

- Isolated risk management can produce purely qualitative assessments that can lose the ability to be compared over time due to a lack of standardization. Qualitative assessments do not always readily fold into compliance or business continuity programs without requiring some conversions into "quantified" outputs. Assigning subjective numbers to high, medium, and low scales does not eliminate the need to assign asset values and safeguard cost figures, as business impact calculations are often based on these figures.

- Isolated compliance management can produce a mix of metrics based on what was able to be measured, as opposed to what needs to be measured. Over time, this can result in unused or ignored measurements while missing the more interesting metrics.

- Isolated business continuity management can produce incomplete business continuity management programs that stall with untested IT disaster recovery plans or with a few business impact assessments for some of the organization's applications. These programs can fall short of establishing both comprehensive and tested plans that support business survivability during a disaster while fully integrating security.

Enterprise, Holistic Approach

A more robust approach is to integrate these four programs. The Cisco Global Government Solutions Group's security framework is built on a foundation of security domain elements derived from industry-recognized best practices and defined as security policy requirements. Figures 1 and 2 illustrate the security framework and security policy domain elements, respectively.

Figure 1: Security Framework

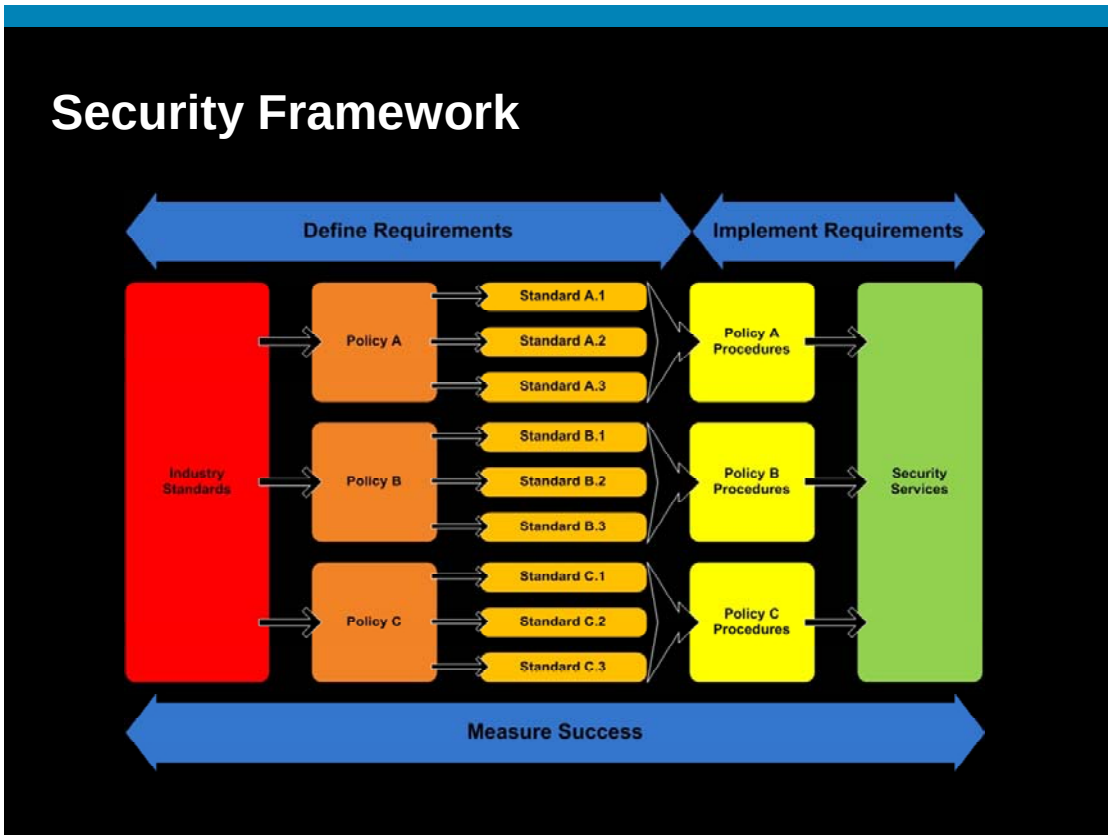
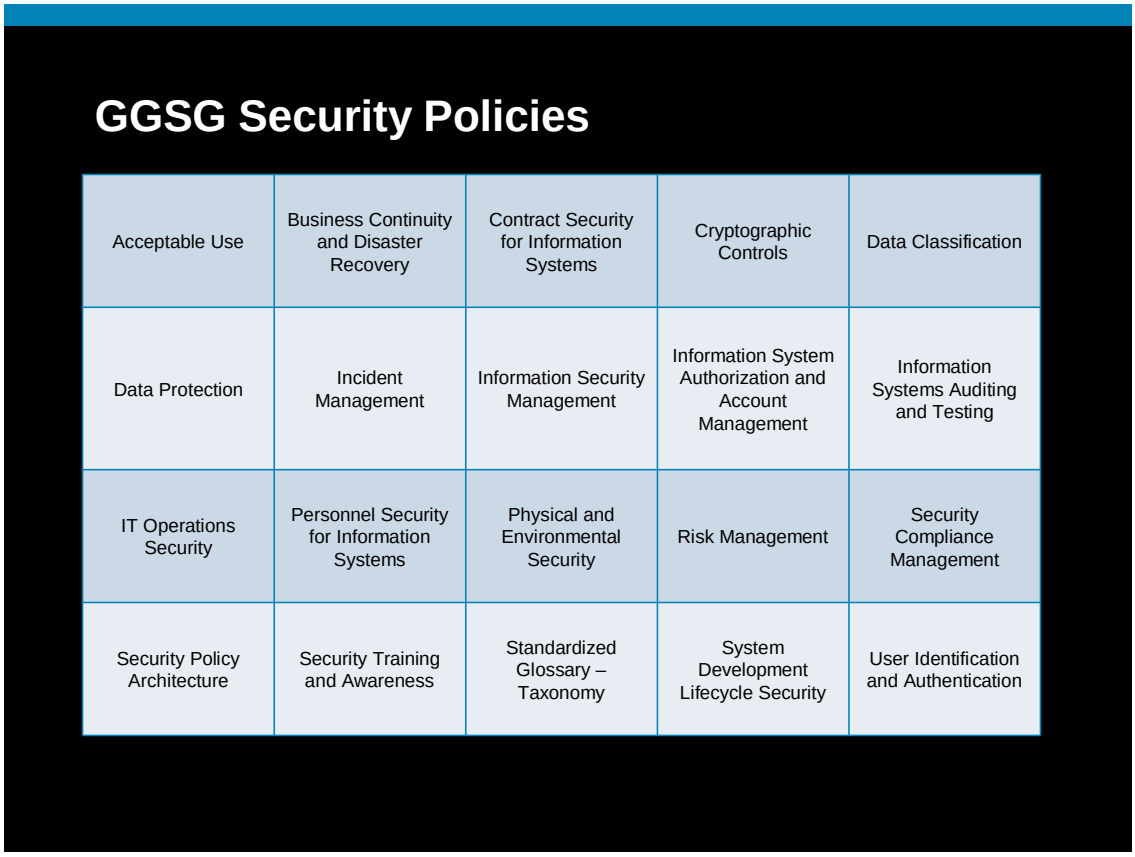


Figure 2: Security Policy Domain Elements



The group's security policy elements map directly to the ISO17799/27002 and NIST SP800-series codes of security practice. These two standards provide broad coverage across a range of technical, physical, and administrative controls and establish an anchor point to be used to relate to other industry standards such as ITIL, CoBIT, COSO, SOX, etc.

Figure 3 shows the Cisco Global Government Solutions Group integrated security framework. The integrated framework clearly illustrates what the organization's requirements are (on the left), how the requirements are being implemented (in the middle), and with risk and CMM measurements of the current implementation of each element (on the right).

Figure 3: Cisco Global Government Solutions Group Integrated Security Framework

GGSG Integrated Security Framework- End-to-end mapping examples

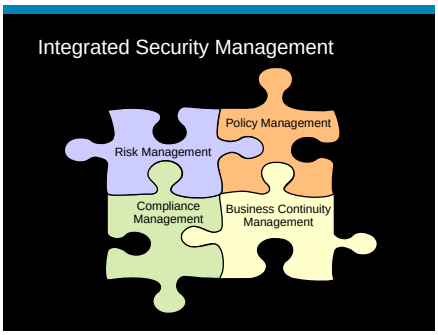
Define Requirements			Implement Requirements			Measure Success	
Framework	**Policy**	**Standard**	**Procedure**	**Security Service**	**Project Name**	**Risk Ranking**	**CMM Service Delivery Scoring**
▪ **ISO17799** ▪ **NIST SP800**	▪ **Define security policies**	▪ **Define policy standards**	▪ **Define policy procedures**	▪ **Define security services**	▪ **Map projects to security services**	**Risk ranking**	**Project/service delivery scored using CMM**
▪ **ISO17799** 11.02 11.04.02 11.05.02 ▪ **NIST SP800** IA-(1,2)	▪ User Identification and Authentication Policy	▪ **Utilize native Active Directory authentication mechanisms**	▪ **User must authenticate to GGSG IAM for enclave access**	▪ **Trusted Identification** ▪ **Authentication**	▪ **GIAM – enclave authentication designs**	**High**	**Ident.= 2 of 3 Gap =1** **Authent.= 2 of 4 Gap = 2**
▪ **ISO17799** 10.10.01, etc. ▪ **NIST SP800** AC-1, AT-1, etc.	▪ Security Compliance Management Policy	▪ **3-tiered metrics**	▪ **Procedures to implement metrics**	▪ **Assurance**	▪ **Desktop compliance automation**	**High**	**Assura.= 1 of 3 Gap = 2**

Integrated Approach

Policy, project, and risk relationships can be seen in Figure 3. Given that we assess risk for all assets during enterprise risk management, we can simultaneously fulfill another risk assessment requirement by using the risk scores for critical assets, relevant to business continuity/disaster recovery planning. This reduces the need for duplicating risk assessment efforts and helps to standardize risk analysis across previously separate risk and business continuity management programs.

Compliance management ties into the framework on multiple levels. First, a gap analysis against the security framework's requirements highlights missing elements in the organization's security program. Second, it shows the extent that specific requirements to an industry standard have been met for certification purposes.

Figure 4: Integrated Security Management



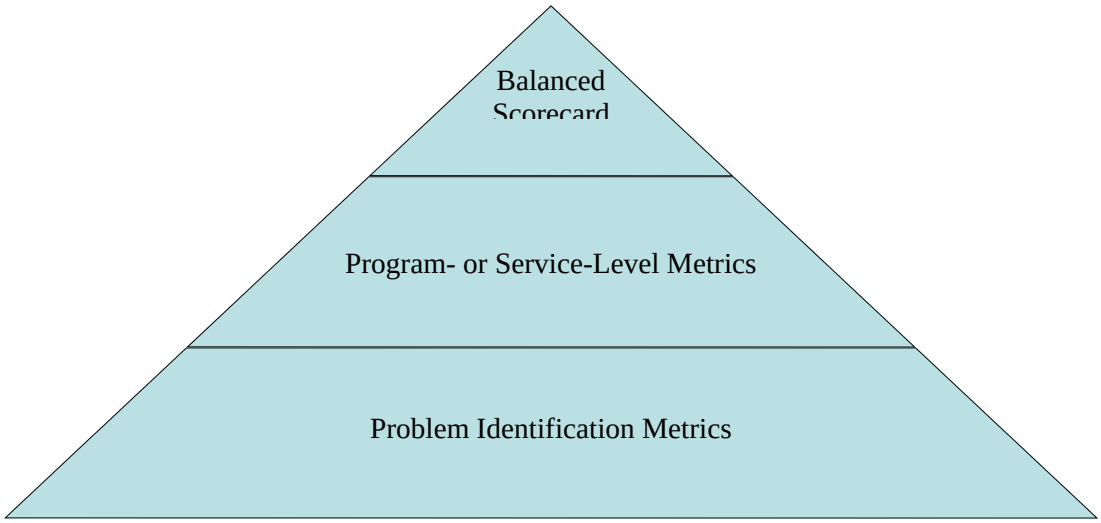
Compliance management (Figure 4) also helps ensure that only standardized, enforceable policies are published. For example, an organization can define compliance to a business continuity policy requirement as both maintaining updated business continuity/disaster recovery plans, and periodic testing of these plans to support the survivability of the business in a disaster.

Measuring Success

Compliance should be both measured and reported to give decision makers an honest assessment of an environment. Similar to reactive policy development, unplanned metrics development can result in too many scorecards. In *Security Metrics: Replacing Fear, Uncertainty and Doubt,* author Andrew Jaquith recommends focusing metrics efforts on meaningful measurements. To learn more about this book, visit http://www.amazon.com/Security-Metrics-Replacing-Uncertainty-Doubt/dp/0321349989.

Agreeing upon a tiered system of metrics allows an organization to track what is interesting by focusing on what supports the mission. The Global Government Solutions Group's metrics are made up of three levels (Figure 5).

Figure 5 Metric Levels



At the lowest level, measurements enable problem identification, such as system uptimes or percentage compliance to a set of standard system configurations. At the program level, metrics measure solution effectiveness, such as customer satisfaction ratings, risk, and CMM service delivery scores.

Lower-tiered metrics could be made up of:

- System uptimes
- Percentage compliance to desktop or system standards
- Time to close trouble tickets or cases
- Number of vulnerabilities detected and resolved
- Employee turnover rate
- Percentage of employees that completed required security training
- Solution ROI scores measured using quantitative risk management
- Number of spam emails or network probes blocked

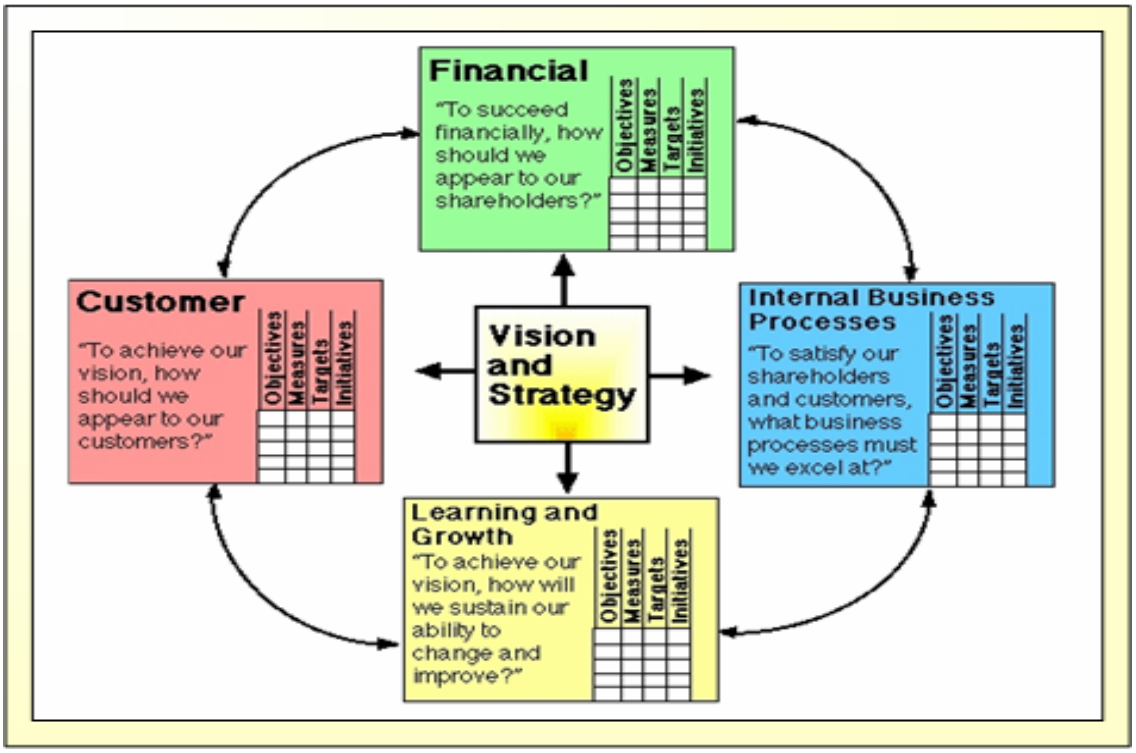
The top tier provides a simple interface representation to the business and is based on an industry -recognized concept of the balanced scorecard, made up of four perspectives (Figure 6):

- Learning and growth
- Internal business process
- Customer
- Financial

http://en.wikipedia.org/wiki/Balanced_scorecard

The balanced scorecard helps provide a more comprehensive view of a business, which in turn helps organizations act in their best long-term interests. Executives get this broader set of metrics representing the health of the organization by bringing up metrics of interest from the lower tiers.

Figure 6 Balanced Scorecard



An example scorecard could be made up of the following metrics:

- Ratio of contract vendors to regular employees
- Combined CMM scored and risk-rank ordered business processes
- Customer satisfaction score
- Business unit cash flow

Conclusion

Implementing an integrated security framework provides efficiencies between security policy, risk, compliance, and business continuity management programs. Security practitioners can quickly show the corresponding business risk addressed by each element of the security framework. They can also measure and report on how each IT security service is delivered across the framework.

Beginning with industry recognized standards as the foundation to the organization's security architectural framework provides:

- Comprehensive, holistic security governance
- A flexible framework that can be applied to other standards such as SOX, CoBIT, ITIL, PCI, NIST, etc.
- Clear relationships between the framework's elements
- Reduced overall policy development and risk management efforts

Comprehensive risk assessments against security framework requirements identify risks to the organization and can also be used to identify gaps in security policy, regulatory compliance, and industry standards compliance. This reduces parallel efforts and supports standardization for comparisons over time. These assessments also feed business impact analysis efforts for business continuity management, thus eliminating the need for duplicate risk surveys from business continuity/disaster recovery teams.

Additionally, more complete asset inventories can be maintained. By building asset valuation and criticality rankings into the project life cycle (PLC) process for the provisioning of new equipment, services, and applications, this data is collected up front as a distributed yet standardized effort throughout the organization. Embedding security governance into business processes solidifies the overall security posture in a more proactive and cost-effective way, which can evolve as the business evolves.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-375487-00 10/06