The Risk Management Framework: Building a Secure and Regulatory Compliant Trading Architecture

Introduction

Enterprise architectures in financial institutions are traditionally built around functional and operational requirements. Security and regulatory compliance needs are typically addressed by individual business and technology groups, which often results in overlapping solutions, functional gaps, or both. As security and regulatory compliance activities have evolved into vital business elements with cross-functional data requirements, these architectural inefficiencies have become business liabilities. The lack of ready access to a consistent, enterprise-wide plan adds costs, delays services, and complicates management as businesses work to implement new compliance requirements.

Cisco has created an integrated architecture framework that fuses today's functionally capable and operationally reliable trading floor architectures with the components required for security and compliance. It supports comprehensive, enterprise-wide solutions that reduce unnecessary overlap, and provides a foundation for addressing new regulations as they arise. This paper defines our Functionally Capable, Operationally Reliable, Regulatory-Compliant, Secure (FORS) framework, and describes how Cisco® and partner solutions for the financial industry work within that framework to meet the demanding requirements of today's trading environment.

Risk Management Demands Architecture Update

It's possible that the "FUD" (fear, uncertainty, and doubt) factor has never been such an apt characterization of the financial industry. Sub-prime write-downs have resulted in highly volatile and unpredictable market conditions. Exchanges and market venues around the world are consolidating to remain competitive. Financial markets are globalizing at a rapid pace. According to a 2006 Securities Industry and Financial Markets Association (SIFMA) report, the U.S. share of the global market capitalization fell from 56 percent to 36 percent between 1982 and 2006, while the emerging market capitalization rose from 37 percent to 57 percent during the same time period.

Adding to the challenges of this uncertain and changing environment are mounting incidents of security breach and attempted fraud. The growing security threat has sparked a dramatic increase in the number of regulations and the importance of regulatory compliance. The Gramm-Leach-Bliley Act for retail banking and Regulation NMS (Reg NMS) and Markets in Financial Instruments Directive (MiFID) for financial markets are just a few examples of regulations that government agencies have enacted in response to various security incidents and to keep markets fair to investors. The consequences of failure to comply with government regulations are dire. Noncompliance threatens not only competitive success, but also the very existence of a financial firm.

Today's financial firms depend on technology to address the risks inherent in changing business, security, and regulatory landscapes. Virtually any trading floor architecture can support technology implementations such as improving data capacity and bandwidth, implementing a real-time platform, and developing tools for liquidity discovery. However, two critical technology priorities for

reducing risk must be addressed at the architectural level: building an integrated global risk model, and establishing and implementing an IT governance model.

The traditional approach of separate core and compliance functions is not well suited to implementing risk management at the enterprise level. Business and technology architecture organizations must update and expand enterprise architectures to mitigate risk as they address regulatory and security needs.

A Comprehensive, Integrated Architecture Approach

Today's risk environment for the financial markets industry spans operational, credit, market, security, and regulatory compliance issues. Firms are realizing that they need to build an integrated, modern service management environment that addresses all aspects of business and technology. The most effective way to accomplish that goal is through a comprehensive, integrated enterprise architecture approach.

Most successful financial firms have the advantage of starting this process with strong and mature architecture mechanisms for managing functional and operational needs. Functional systems meet the business needs required to compete successfully, and operational systems meet the day-to-day requirements for availability, reliability, and recoverability.

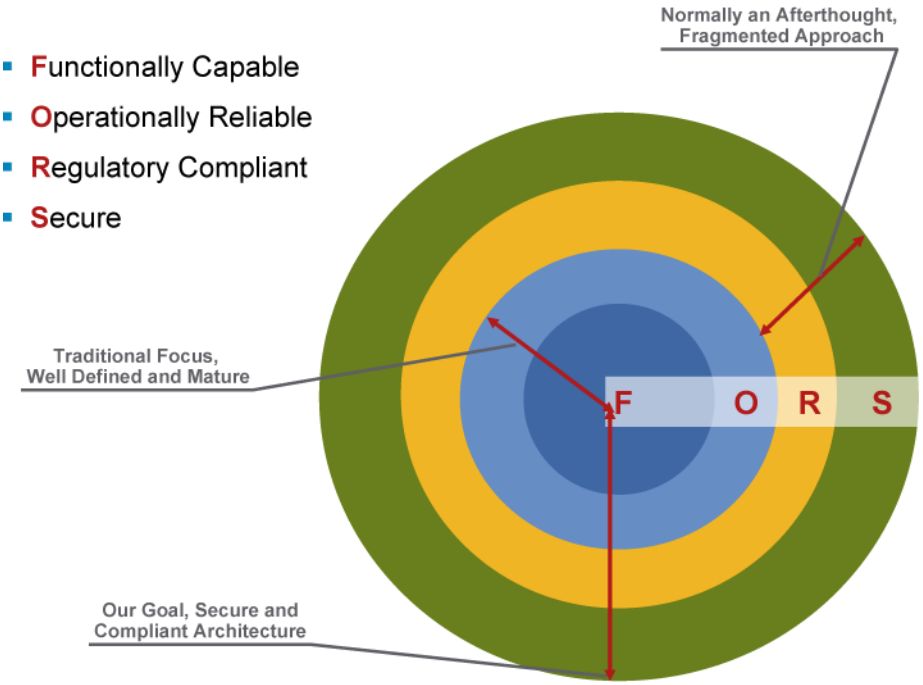
Going forward, firms must integrate their functional and operational architecture development process with the security and regulatory compliance initiatives that traditionally existed within multiple individual organizations throughout the enterprise. The regulatory compliance element will address the industry rules and regulations of different countries, and the security element will provide a safe environment for employees and business partners to conduct business transactions. These elements must be integrated into the core architecture without detracting from the existing functional and operational architectural strengths, so firms remain competitive. Combining all of these dimensions into a strong and cohesive architecture will:

- Help mitigate risks (market, credit, operational, reputation)
- Facilitate compliance with government regulatory requirements
- Provide the functional capabilities needed to compete in a regulated marketplace
- Support secure trading transactions and interactions within the enterprise, with customers, and with business partners
- Protect the firm's critical assets (customer information, corporate information, intellectual property, and infrastructure)
- Provide efficient security and compliance monitoring, operation, management, and reporting to regulatory bodies

Cisco's Vision: The FORS Model

The FORS model is a framework for creating trading floor architecture with four critical domains: functional, operational, regulatory, and security (Figure 1). The framework focuses on the interdependencies among these architecture domains, and uses a holistic, Enterprise Architecture approach to reduce overlaps and minimize capability gaps across the whole enterprise. Using the FORS framework can help ensure that the architecture community addresses regulatory and compliance needs every time the functional and operational architectures are updated, and also addresses functional and operational needs during security and compliance updates.

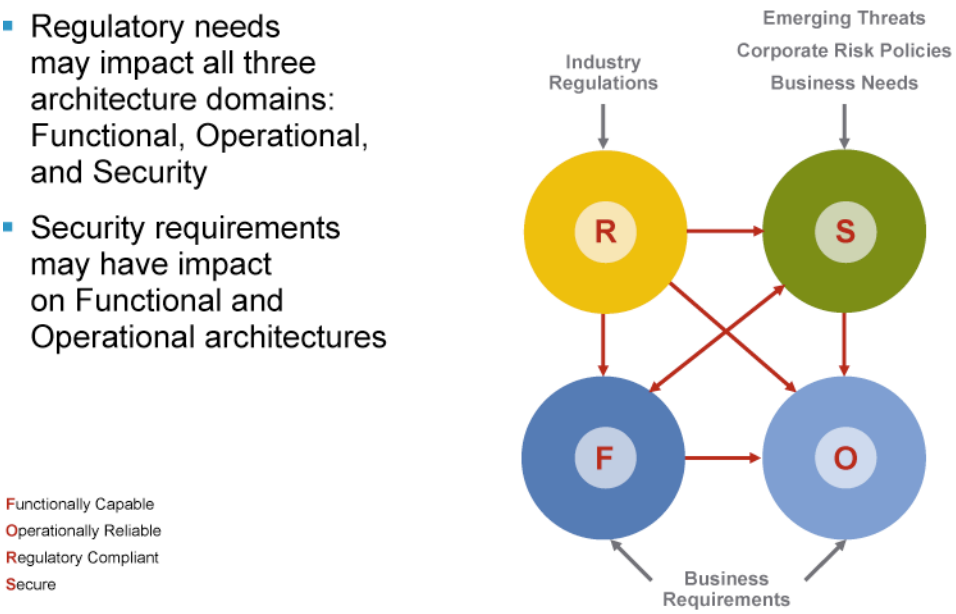
Figure 1. The FORS Model



Interdependency among the Architecture Domains

The functional, operational, regulatory, and security domains of financial enterprise architectures are interrelated (Figure 2). Architecture developers need to understand and address the functional and operational interdependencies as they expand the traditional core focus to encompass security and regulatory compliance. Assuring compliance and mitigating risk involves all four domains.

Figure 2. Interdependency among Architecture Domains



Regulatory Interrelationships: Regulatory compliance requirements may impact any or all of the functional, operational, and security architecture domains. However, the impact on these domains may differ from regulation to regulation. For example, Reg NMS has a significant impact on the functional and operational domains. It requires firms to have low-latency systems for best execution, which affects the operational domain, and to handle a large amount of market data from multiple sources, which affects the functional domain. In contrast, the multi-factor authentication requirements of the Gramm-Leach-Bliley Act and the role-based identification and access management requirements of the Sarbanes-Oxley Act have more impact on the security domain.

Security Interrelationships: The security domain has a bidirectional relationship with the regulatory compliance, functional, and operational domains. Security needs may impact these domains or may be impacted due to changes in these domains. For example, in the case of wireless and mobility solutions, security issues have slowed the adoption of wireless while security architectures have been enhanced to support wireless deployment.

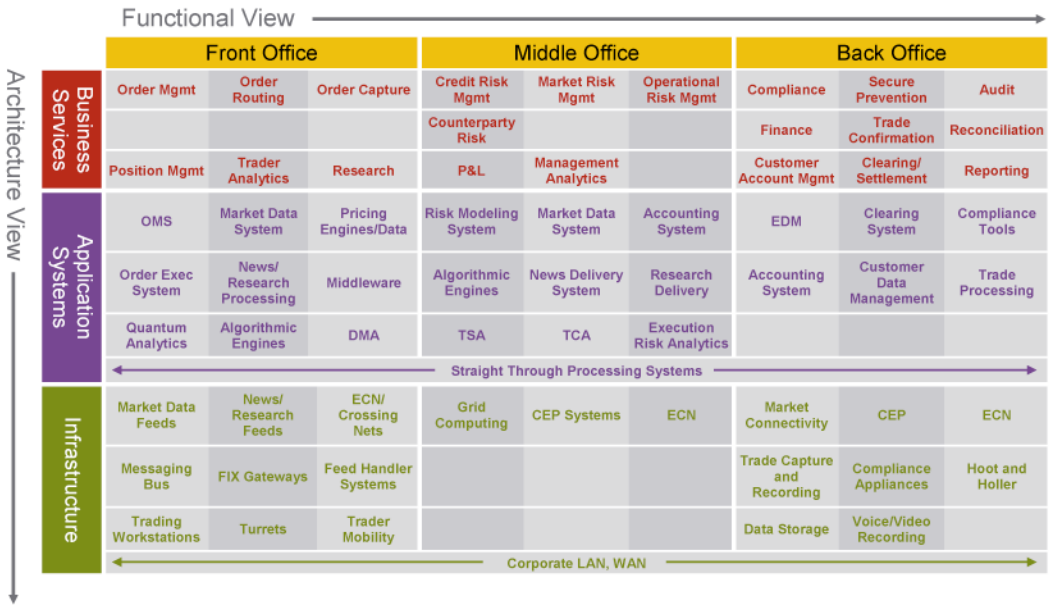
Holistic Approach

The second major component of the FORS framework is a holistic Enterprise Architecture approach based on The Open Group Architecture Framework (TOGAF), an industry standard that includes all business and technology aspects of an enterprise. A high-level, top-down approach is vital when assessing the end-to-end enterprise impact of any change in business needs and modifying and aligning the relevant architectures. Different regulatory concerns may impact business and technology systems in similar manners, resulting in overlapping requirements for different regulations. Without a holistic view, similar or duplicate solutions could be deployed for different regulations, or some of the required capabilities might be overlooked.

Figure 3 shows how the Enterprise Architecture approach helps to create an end-to-end view of a typical trading environment. This view has several benefits, which include:

- Providing a complete functional and architectural picture of the trading environment
- Helping align business needs with applications and infrastructure
- Providing a baseline view that can be used to assess the impact of functional and architectural changes between front, middle, and back offices

Figure 3. Enterprise Architecture View of a Trading Environment



Applying the FORS Model

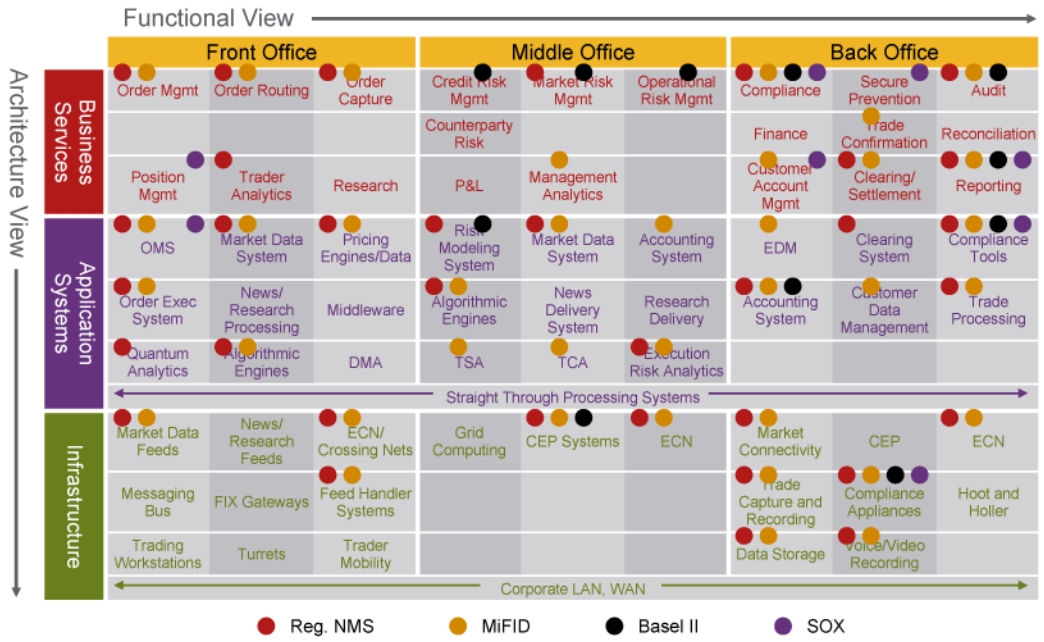
The balance of this paper will focus on using the FORS model to identify the impact of current financial market regulations and security needs, and developing a corresponding architecture and solution set. Understanding how the FORS model is applied also helps to illustrate the value of using an integrated framework today and how that framework can be applied to future regulatory and security needs.

Regulatory Compliance

Many regulations affect the financial services industry. This paper examines four major regulations that have a significant impact on the trading environment: Reg NMS, MiFID, Sarbanes-Oxley, and the Basel II Accord.

Applying the FORS model to these four regulations clearly shows their affect on various business processes, application systems, and infrastructure in the front, middle, and back office areas of the trading floor (Figure 4). Examining regulations' end-to-end impact is extremely important because regulations tend to affect almost all areas of business and technology, and multiple regulations may have similar requirements. An end-to-end examination can present opportunities to reduce costs and increase operational efficiency by using solutions for multiple purposes instead of duplicating investments.

Figure 4. The Impact of Regulations on the Trading Environment



Mapping the impact of each regulation to the trading environment helps in identifying the various controls required for compliance. The controls can include people, process, and technology, and can differ subtly between regulations. For example, ensuring best execution for Reg NMS requires only a best price guarantee, while ensuring best execution for MiFID may include all the costs associated with that trade. Figure 5 shows the controls that are required for compliance to the four major regulations.

Figure 5. Controls for Regulatory Compliance

Regulations	Front Office	Middle Office	Back Office
Reg. NMS	▪ Ensure Best Execution Order Execution Rules Market Data Latency Market Data Rules (NBBO) Access to market venues ▪ Written Procedures and Policies for trade execution	▪ Market Risk Controls Include Best Execution ▪ Operational Risk Controls Pricing data latency Cross venue capability ▪ Written Procedures and Policies for risk management	▪ Regulatory Reporting ▪ Prove Best Execution Trade Archival Seven-day pricing data history ▪ Compliance Monitoring processes and tools
MiFID	▪ Customer Classification Rules ▪ Ensure Best Execution Order Execution Rules Market Data Latency Access to market venues ▪ Written Procedures and Policies for trade execution	▪ Market Risk Controls Include Best Execution ▪ Operational Risk controls Pricing data latency Pre-trade TCA ▪ Written Procedures and Policies for risk management	▪ Trade Reporting Report trade in three minutes ▪ Prove Best Execution Trade Archival for five years Reconstitute trade ▪ Compliance Monitoring processes and tools
Basel II	▪ Fraud Detection and Control—Internal/External	▪ Operational Risk Controls Measure and quantify economic value across seven risk areas End-to-end transactional risk	▪ Vulnerability Assessment Real-time measurement of security controls and processes
SOX	▪ Identity Management and Access Control People to Applications Applications to Applications	▪ Identity Management and Access Control People to Applications Applications to Applications	▪ Identity Management and Access Control People to Applications Applications to Applications ▪ Auditing and reporting of all controls

To understand the impact of a particular regulation on the enterprise infrastructure and the corresponding need for controls, let's look at Reg NMS. Reg NMS impacts the way that firms can execute orders because it requires that firms execute a particular order at the best market price.

In the front office, Reg NMS primarily impacts the order management and execution functions. Order execution rules may need to be modified to help ensure that no trade through occurs for limit orders. The market data and access rules may need to be modified to help ensure fair and nondiscriminatory access to quotations. Firms must modify these rules to implement best execution. At the infrastructure level, the market data systems must operate with minimum latency so they can obtain the most recent pricing information from the market. Also, to obtain all the market pricing for particular instruments, the market systems need expanded access to market venues and must be able to handle more data.

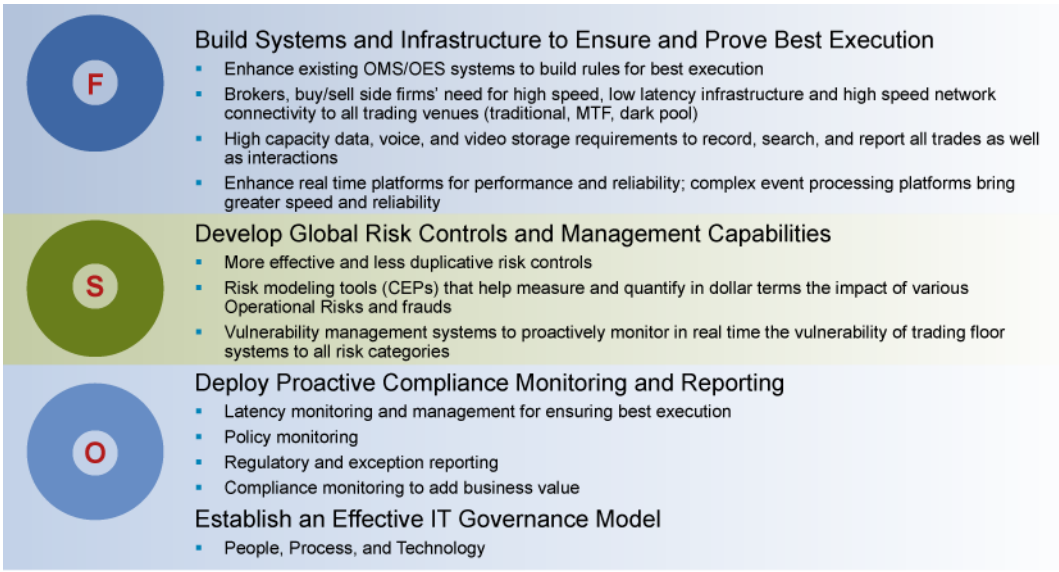
The need for written policies and procedures regarding the best execution of rules poses yet another new requirement. Firms not only need to comply with Reg NMS, but to document their compliance.

The middle-office requirements include added risk management capabilities. For example, firms must address a new type of operational risk called execution risk, which addresses the failure to execute an order at the best price.

In the back office, procedures must be modified to not only ensure best execution, but to prove that trades were executed at the best prices. If asked, firms must provide at least a 7-day pricing history, which requires reliable archiving of trade executions. Back-office requirements also include compliance monitoring. From the operations perspective, the risk management groups in all organizations must modify their compliance monitoring tools and processes to include the various requirements for Reg NMS.

Figure 6 shows the incremental requirements that trading floor architectures must incorporate to address the impact of regulations, based on the controls detailed in Figure 5. This figure shows that these regulations impact the functional, operational, and security domains of the framework—providing additional evidence that an integrated approach such as the FORS framework is necessary for a comprehensive architecture.

Figure 6. Architectural Impact of Regulations



Security

This section will discuss applying the FORS model to the specific security needs of the trading environment.

The increased use of networking and online tools, combined with the growing volume of trading activity, has made the trading floor environment more vulnerable and difficult to protect. Financial firms not only have more data at risk, but also suffer greater consequences if that data is lost or compromised. Attacks such as spyware, viruses, and identity theft can be devastating –impacting clients' financial health and potentially damaging a firm's reputation beyond repair.

The trading floor architecture must protect users from a wide and growing variety of security threats, and that protection is most effective when it is ingrained in the enterprise architecture. The FORS model can be readily applied to the four major drivers that define the security architecture of an enterprise.

- **Business needs:** As business models evolve, driven by technology, information security becomes critical.
- **Emerging threats:** New and increasingly sophisticated threats need to be addressed.
- **Corporate risk policies:** Corporate policies drive the definition of risk profiles of critical assets.
- **Regulatory requirements:** Many regulatory requirements impact security requirements.

Once security threats are understood, the appropriate controls can be implemented. Figure 7 maps the security controls required to mitigate various security threats and again validates the importance of using an integrated approach such as the FORS framework.

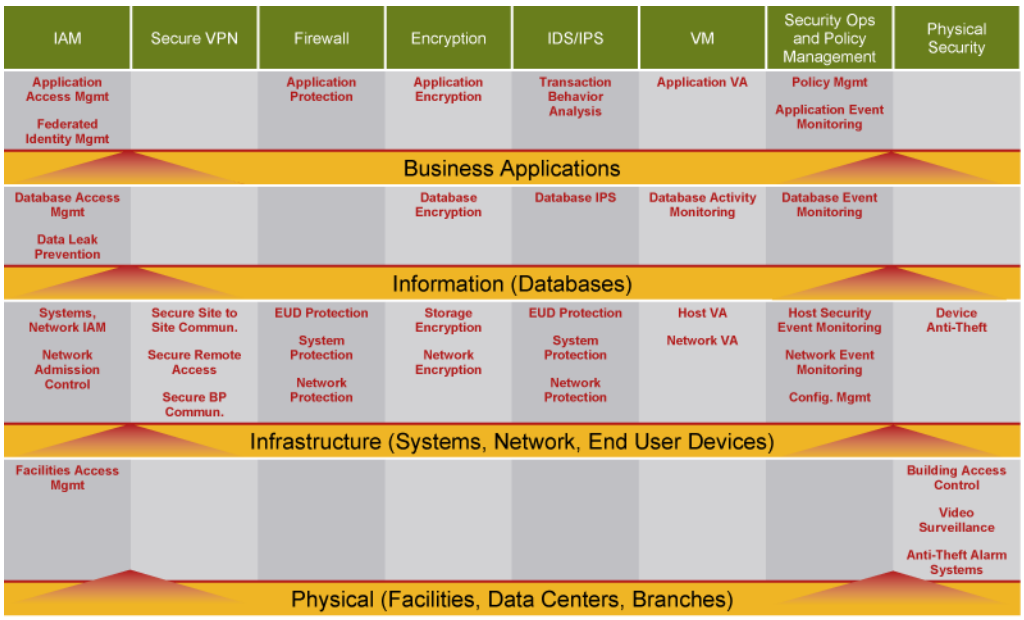
Figure 7. Security Controls for Threat Mitigation and Regulatory Compliance

	Threats								Regulatory Compliance*			
Security Controls	Virus, Worms, Spyware, Spam	Employees Acting in Unauthorized Ways	Poor Protection of Information Assets	Denial of Service	Phishing	WLAN Threats	Identity Theft	Zero Day, OS Threats	GLB	Sarbanes-Oxley	Basel II	FFIEC
Firewall	✓	✓	✓	✓	✓	✓		✓		✓		
Identity and Access Management	✓	✓	✓			✓	✓	✓	✓	✓		✓
Encryption			✓			✓	✓		✓			✓
IDS and IPS	✓			✓	✓			✓	✓		✓	
Secure VPN			✓			✓	✓					
Vulnerability Management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Physical Security		✓	✓				✓					
Security Operations and Policy Management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

*The ones shown here have direct relevance to security services

The security controls and architecture requirements for the financial services industry have been described in detail in another Cisco white paper titled, "Unified Security Architecture for Financial Services". The security services and controls discussed in this paper are also fully applicable to the trading environment. Figure 8 shows how each of the security services contribute to securing all the business and technology areas of a financial services firm. Most of the security services are architected at the infrastructure layer as shared services that protect other layers of the enterprise. Security services architected at the infrastructure layer must be able to meet the varying security needs of enterprise-wide applications.

Figure 8. Security Risk Controls—Enterprise Architecture View

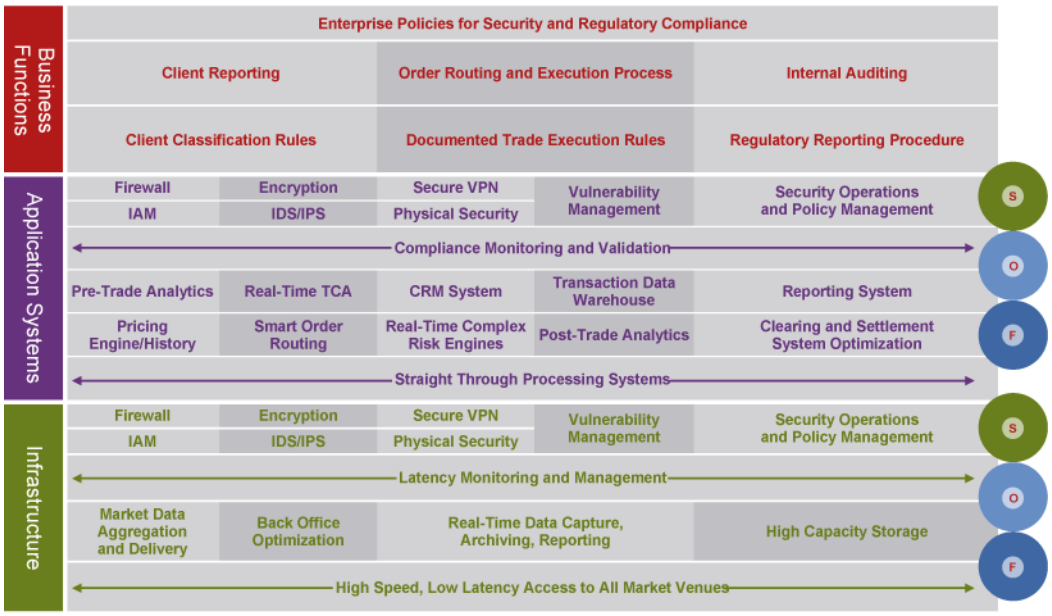


Source: Unified Security Architecture for Financial Services, by CH Hariharan, Anuj Kumar

Incremental Architecture Updates

Figure 9 shows the incremental capabilities required to make an enterprise trading floor architecture regulatory-compliant and secure. Regulatory compliance may require changes in the functional, operational, and security dimensions of the Enterprise Architecture. From improving the process of reporting trades and data warehouse systems for client classification, to supporting increased storage requirements for data and trades, to enhancing application systems with resources such as real-time, complex risk engines and smart order routing, to better risk modeling and security, the entire end-to-end architecture must be revisited and updated. These incremental steps become more effective and easier to architect and administer within a consolidated architectural framework.

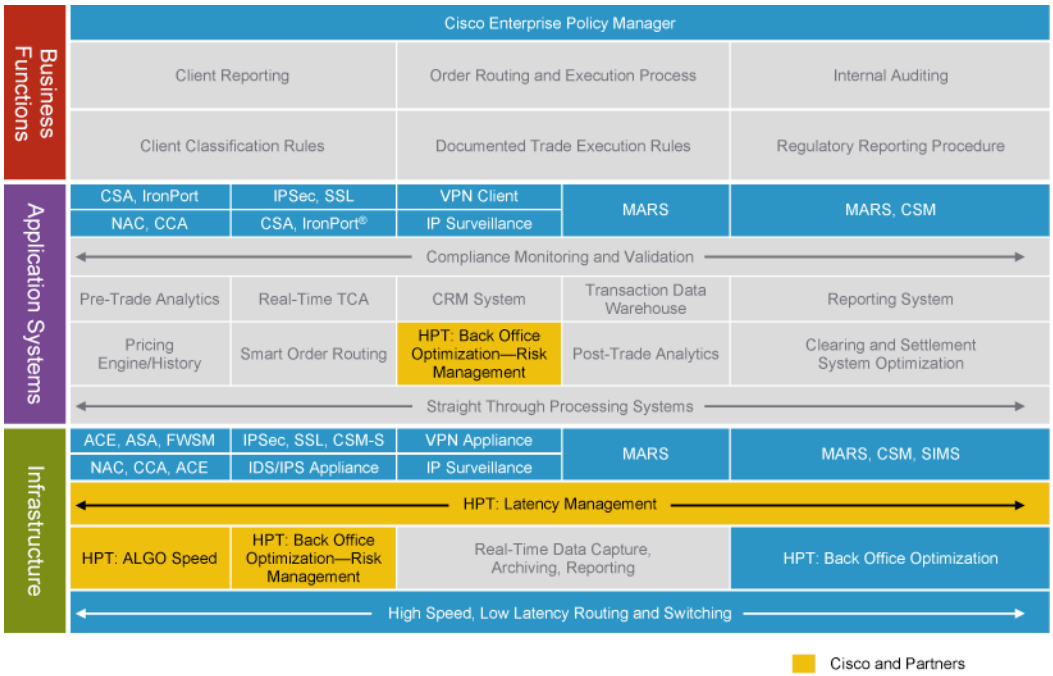
Figure 9. Incremental Architecture Capabilities Required for Security and Regulatory Compliance



Cisco and Partner Solutions

Cisco and its partners offer a wide range of infrastructure and application system solutions that can help financial firms create a secure and compliant architecture (Figure10).

Figure 10. Cisco and Partner Solutions



In addition to offering traditional network and security products, Cisco has invested in technology and partnerships to develop the next-generation trading infrastructure, resulting in a modular set of offerings that comprise the Cisco High-Performance Trading (HPT) solution portfolio. This portfolio can help firms build a highly available, modular, scalable, and low-latency infrastructure to handle

the exponentially increasing volumes of market data and trades. Three solutions are especially relevant to compliance challenges:

- **The Algo Speed** solution supports low-latency trading for the automated front office, which helps firms fulfill the best-execution requirement. The main features of this solution are sub-millisecond (ms) application latency, and microsecond fabric recovery and failover around link failures. Another important feature is latency monitoring with microsecond granularity, which facilitates best-execution tracking.
- **The Back-Office Optimization—Risk Management** solution focuses on improving the response time of risk management applications to facilitate better risk assessment without delaying the flow of trades.
- The Latency Management solution provides latency analytics at the microburst level across the entire trading cycle to help firms track and record the latency for various execution venues, which is critical for best-execution requirements.

For additional information about specific solutions and products, please visit http://www.cisco.com/go/financialmarkets.

A Secure and Regulatory Compliant Trading Architecture

Risk management is critical for any financial firm. As security and regulatory compliance are central to managing risk, integrating security and compliance capabilities into the enterprise architecture should be a significant part of a firm's technology priorities.

Despite the massive use of technology in business processes, the need to develop technology architectures that cope with regulatory requirements and security breaches has not been recognized in a systematic way. To protect their own and their clients' assets, financial firms—and particularly those firms in the trading industry—must integrate security and compliance capabilities into the core trading floor architecture.

The integrated FORS framework can help firms expand an existing architecture to address security and compliance requirements, and implement solutions from Cisco and its partners that are aligned across the infrastructure, application systems, and business functions. Using this structured, end-to-end approach can help firms create a strong foundation that addresses the current and future regulatory and security needs of the trading floor environment.

References

The following is a partial list of references used in researching and writing this paper:

- Unified Security Strategy and Architecture for Financial Services, By CH Hariharan, Anuj Kumar
- Trading Floor Architecture—Cisco white paper
- Design Best Practices for Latency Optimization—Cisco white paper
- Cisco products and technologies white papers
- Cisco SONA framework
- 2008 Trends to Watch—Financial Markets, a Datamonitor report
- Top Priorities in Security and Investment Industry, 2008, TowerGroup
- Reg NMS—Impact on Market Data, Reuters white paper
- Regulation NMS—Be Careful what you wish for, TabbGroup

- MiFID—Impact on US Operations, Capco
- MiFID—the Challenges Ahead, Bearing Point
- MiFID—The Client Management Opportunity, Deloitte
- Market Data Strategies in response to Reg NMS and MiFID, Datamonitor
- Overall Impact of MiFID, Financial Services Authority (FSA) white paper
- Joint Implementation Plan for MiFID, FSA
- BASEL II
- Sarbanes-Oxley Act
- California Security Breach Senate Bill

About the Authors

Anuj Kumar, Enterprise Architect in the Financial Services Advisory group

Contributors:

Mihaela Risca, Global Solution Manager for Financial Markets

Peter Robin, Director IBSG

Parm Sangha, Sales business Development Manager

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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 C11-521656-00 2/09