FIS RISK, INFORMATION SECURITY AND COMPLIANCE (RISC) OVERVIEW

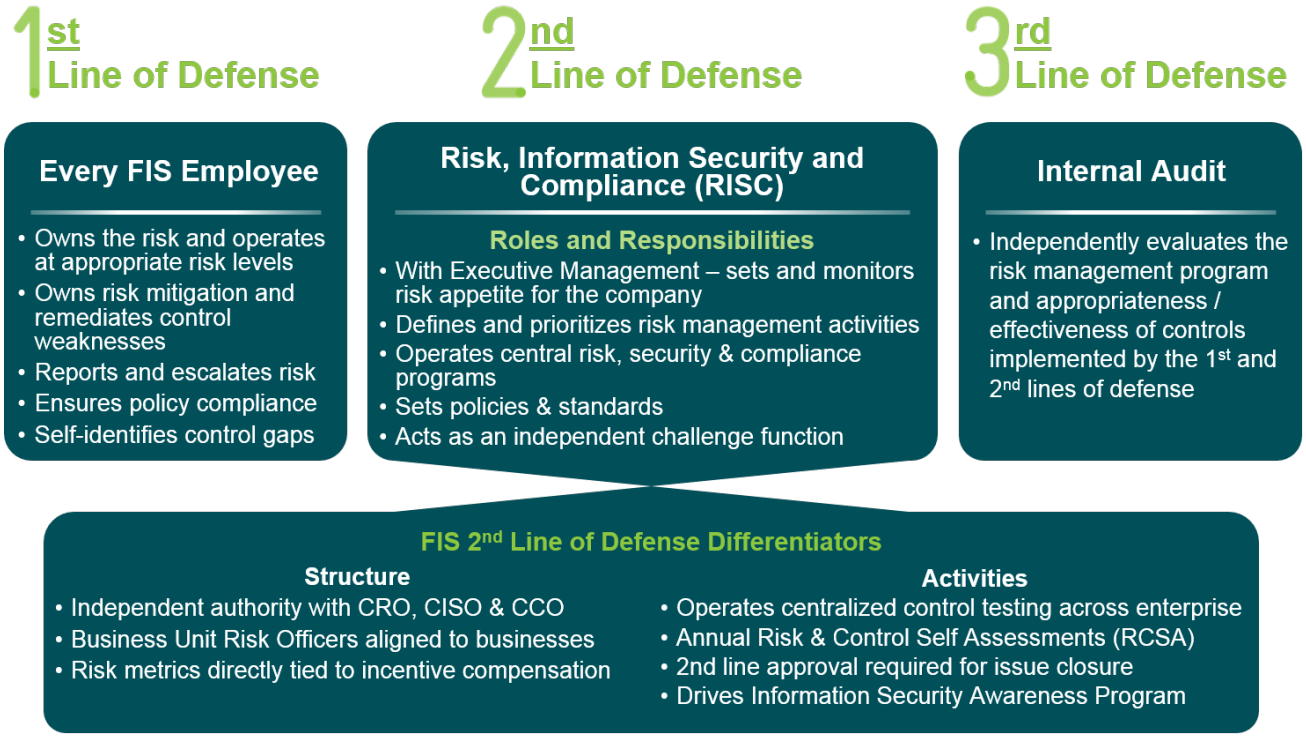
Introduction

The purpose of this document is to describe:

- How the Risk, Information Security and Compliance (RISC) organization fits into FIS' Three Lines of Defense model
- The RISC Organization
- FIS' RISC Programs
- FIS' Top Five Risks

Three Line of Defense Model

FIS has defined clear roles for risk ownership and oversight through our Three Lines of Defense model:



The three lines of defense model forms a system of accountability for risk management across FIS. The business is our First Line of Defense and is the "risk owner". Business lines have interests in innovation, customer support, and corporate growth, all in a manner that is in line with corporate risk tolerance and our secure by design culture. We've instilled a culture of risk awareness that includes self-reporting risks, issues, and incidents. Business owners are responsible for understanding and foreseeing security and risk implications of their decisions. This culture is modeled at the highest levels of the company.

Our Second Line of Defense is our RISC organization. RISC is responsible for helping the organization understand risks, security issues and regulatory requirements. The RISC organization is a true partner with the First Line of Defense. The Second Line of Defense leverages cutting-edge tools, technologies, and practices to stay up-to-date with and offer protection from the ever-evolving barrage of cyber-threats and threat actors.

©2020 FIS and/or its subsidiaries. All Rights Reserved.

FIS' Third Line of Defense is Internal Audit. Internal Audit serves as the last line of defense in this system of checks and balances. FIS' audit teams are rigorous in examining the effectiveness of the programs and controls put in place enterprise wide. Additionally, the audit teams stay abreast of new best practices, regulatory requirements, and trends in industry requirements; thereby serving as another force helping to continuously improve FIS' security and risk programs.

Risk Management Process

The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives. The purpose of the risk management framework is to assist the organization in integrating risk management into significant activities and functions. The effectiveness of risk management will depend on its integration into the governance of the organization, including decision-making. This depends on support from stakeholders, particularly top management.

The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk. This process is illustrated below.



The RISC Organization

Greg Montana serves as FIS' Chief Risk Officer and heads the Enterprise Risk Management, Information Security, and Compliance (RISC) organization. FIS' Chief Risk Officer reports directly to the CEO and indirectly to the Risk Committee of the Board giving RISC independence from the Lines of Business.

©2020 FIS and/or its subsidiaries. All Rights Reserved.

Over the past few years, we have built a team of leaders and subject matter experts that is best in class in our industry. FIS has assembled a well-seasoned team of security and risk professionals who are considered experts in Security and Risk strategy, technology, process, and sustainability.

Highly-respected professionals drawn from:	
Banking	Bank of America, Citibank, TD Bank, Barclays, Lloyds Banking Group, SunTrust, ING
Industry	Verizon Wireless, Deloitte, PayPal

The group includes approximately 700 dedicated RISC professionals recruited from the government and within the industry. These professionals hold certifications in risk, information security and compliance, such as CISSP, CISM, CISA, CRISC, CGEIT, CRCM, CAMS, NSCP and CEH, as well as business continuity planning and disaster recovery CBCP certifications.

The RISC organization is comprised of the following functional areas:

- Risk Management
  - Business Continuity Planning and Disaster Recovery
  - RISC Policy Office
  - Risk Program Office
- Information Security
  - FIS Security Incident Response Team (FSIRT)
  - Security Architecture and Awareness
  - Security Test Team
- Compliance
  - Corporate Compliance
  - Product Compliance
- Government Relations
  - Regulatory Relations
  - Government and Law Enforcement Relations
- Privacy Office
  - Privacy Officer
- Client Risk Relations



Each functional area operates independently within well-defined roles and responsibilities; as well as collectively to accomplish our goal of being the industry leader for information security and risk management among financial technology service providers, and to be our clients' most trusted partner.

For more information on FIS RISC functional areas see the Control Functions links within this same RISC category of the Vendor Management Resource Center.

©2020 FIS and/or its subsidiaries. All Rights Reserved.

Risk Programs

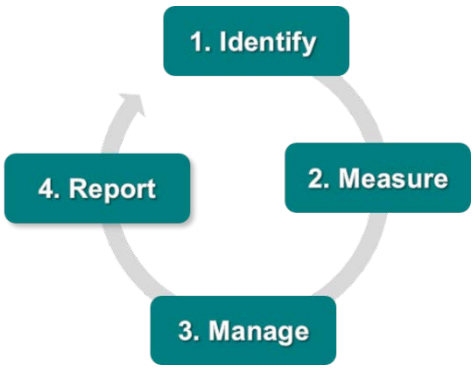
FIS' Risk programs can be organized by function into an IMMR model (Identify, Measure, Manage and Report). Below are a description of each function and a description of the First and Second Lines of defense responsibility for that function.

Identify

Identification programs include monitoring and testing activities as well as risk self-identification processes. The First Line of Defense is responsible for control operation and risk identification while the Second Line provides oversight and challenge of these activities through monitoring and testing. RISC programs include: Control Validation programs, Security Testing, BCP / Disaster Recovery, Vendor Risk Management and Self Identification of Issues.

Measure

Measurement programs take inputs from identification programs and assess risk levels for the purpose of activity prioritization. The First Line of Defense is responsible for setting risk appetite limits and operating within those limits. The Second Line of Defense is responsible for operation of Risk Measurement programs as well as to challenge risk appetite limits and to monitor execution against those limits. RISC programs include: Risk and Control Self-Assessment, Internal loss monitoring, Key Risk Indicators.



Manage

Management programs determine where action is needed, what action is required and how quickly it should take place. The First Line of Defense is responsible for managing risk and remediation of unacceptable risk. The Second Line is responsible for risk governance routines, issue oversight, vulnerability oversight, and policy management. RISC programs include: Vulnerability Management, Governance, Policy Management, Business Unit Risk, and Issue Management.

Report

Regular reporting to executive management and the board enables a performance assessment of our internal controls and governance. The First Line of Defense is the consumer of risk reporting and the Second Line is the producer of risk reporting. Risk produces reporting to be reviewed by the Executive Risk Management Committee as well as the Risk Committee of the Board. RISC programs include: Risk Reporting and Client Risk Relations.

Top Enterprise Risks

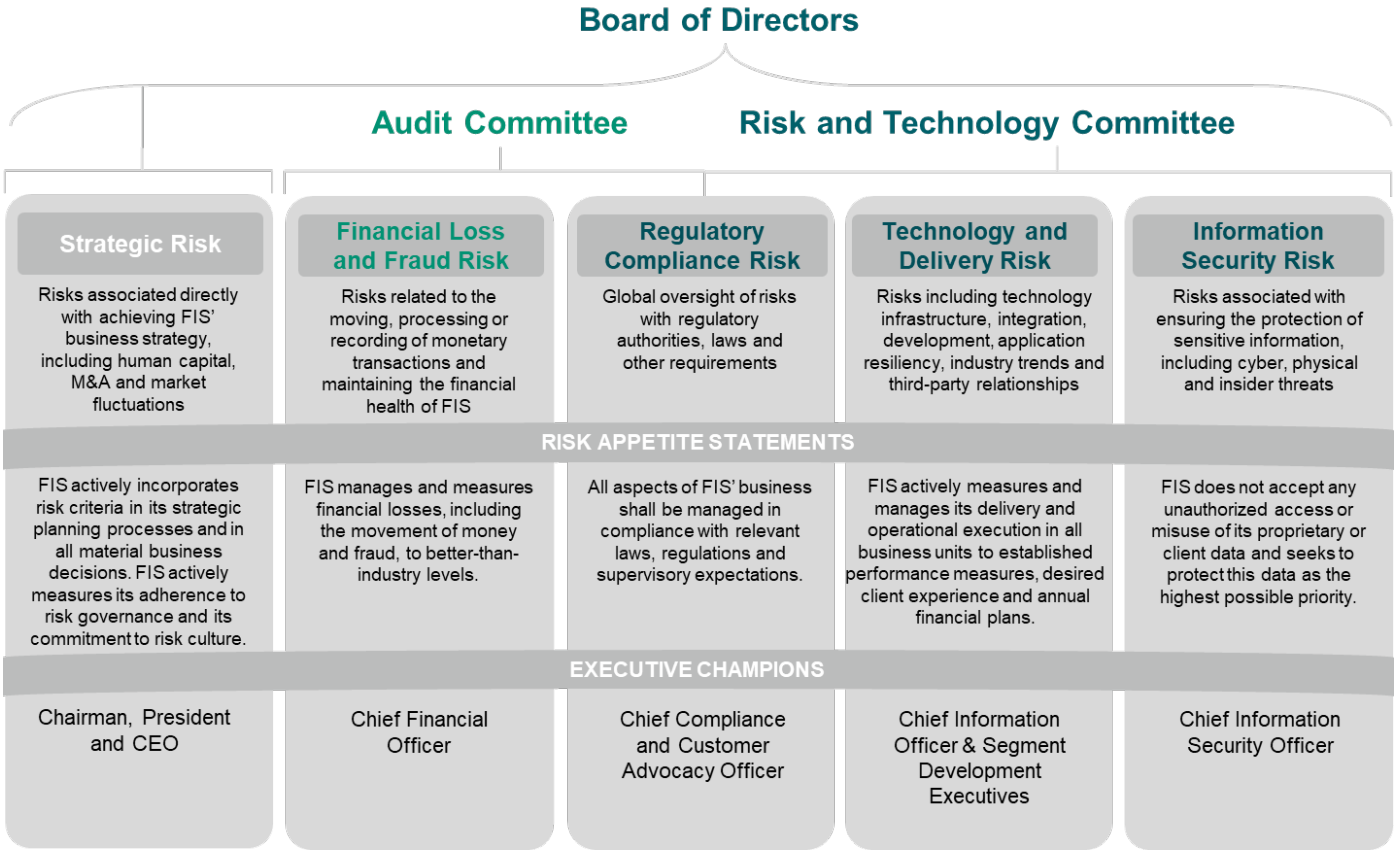
As FIS continues to innovate and serve our clients, we (like all companies) must actively evaluate and manage various risks. This is a task that all organizations face, but the key to successful risk management is the ability to proactively analyze risks across a variety of filters and categories.

Our Top Five Risks serve as the highest level of risk classification and provide the structure for more granular risk classification. All risk activities (Risk and Control Self Assessments, Data Protection Program, Issue Management, etc.) utilize the same nomenclature based on these top 5 risks.

©2020 FIS and/or its subsidiaries. All Rights Reserved.

FIS categorizes and evaluates risk across five major areas:

- Strategic Risk
- Information Security Risk
- Regulatory/Compliance Risk
- Financial Loss and Fraud Risk
- Technology and Delivery Risk



Reputational Risk is viewed as a risk multiplier as there can be a reputational impact to any risk across the top five. The impact of reputational risk is considered for all risks as a component of inhere.

©2020 FIS and/or its subsidiaries. All Rights Reserved.