OPERATIONAL RISK MANAGEMENT:

A GUIDE TO HARNESS RISK WITH ENTERPRISE GRC

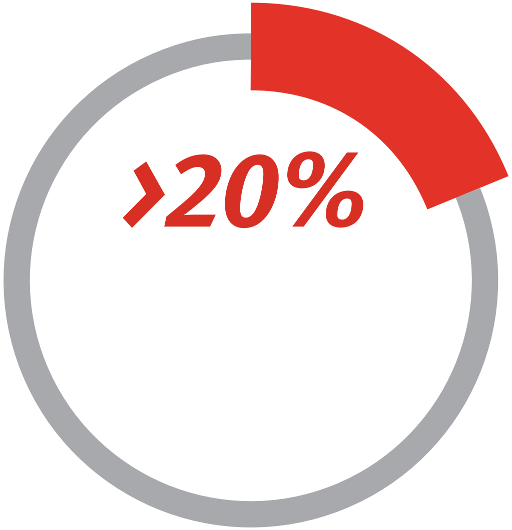
RSA®

TOP RISKS: THE WORLD WITHOUT GRC

LACK OF ENTERPRISE-WIDE VISIBILITY

Every organizational unit has some level of risk it must address. Yet, most internal teams lack the ability to identify priorities and accountability to stay ahead of new threats to the business thus leaving the process of managing risk to be more reactive. While many risks exist within each function, there is often no connected view across the enterprise so business managers often lack visibility into the big picture.

Today, 80% of GRC spend occurs at the department or issue level[1]. If risk is only managed at the departmental level, organizations are left with little insight into other areas of the business. While many organizations are striving to build Enterprise Risk Management (ERM) capabilities, most companies are behind the curve when it comes to actually execution and realizing their goals.



Less than 20% of GRC budgets are spent on top-down enterprise level GRC initiatives.

[1] Source: The GRC Pundit Blog, GRC 20/20

TOP RISKS: THE WORLD WITHOUT GRC

INCONSISTENT VIEW OF RISK

Each line of business within an organization has a different view of risk – from how they identify, assess and manage it to how they monitor and report on it. This results in an inconsistent view of risk across functional areas which can directly impact the overall ability of executive management and the Board of Directors to make effective business decisions and capitalize on new opportunities.

Beyond impairing management's ability to make informed decisions, the inability to provide an accurate view of risk can cause regulators to see an inconsistent treatment of risk. This can lead to more scrutiny from regulators which cost time and resources, or even worse, fines and violations for failing to meet requirements.

In 2013, ***$112 billion*** in new regulations were created which will require organizations to dedicate ***158 million additional hours*** of paperwork in order to comply.[2]

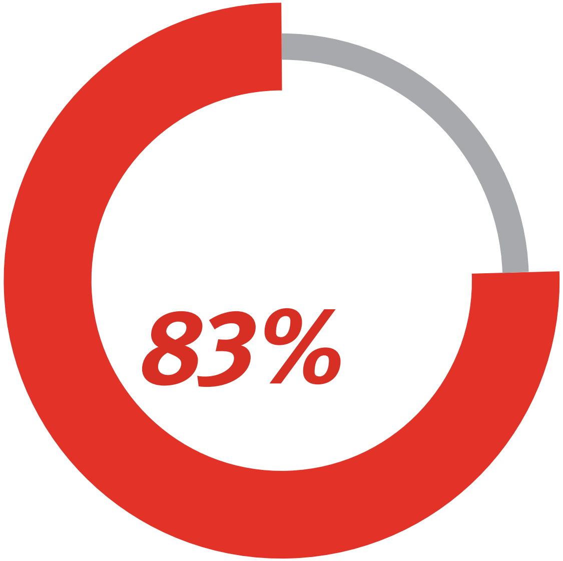
[2] Source: A Regulatory Flurry: The Year in Regulation, 2013, January 2014, American Action Forum

TOP RISKS: THE WORLD WITHOUT GRC

INABILITY TO IDENTIFY UNKNOWN OR EMERGING RISKS

The volume of risk management activities often exceeds available resources. It is difficult already for organizational teams to manage current known risks. By lacking the capacity to better identify unknown or emerging risks, organizations could potentially be put at greater risk if they have no plan to respond to business disruptions.

Cyber risk is a key example of a risk that is dynamic in nature and has wide-reaching impact across several operational units of the organization. Yet, only one in four organizations feel "very confident" in their ability to identify, manage and respond.[3]

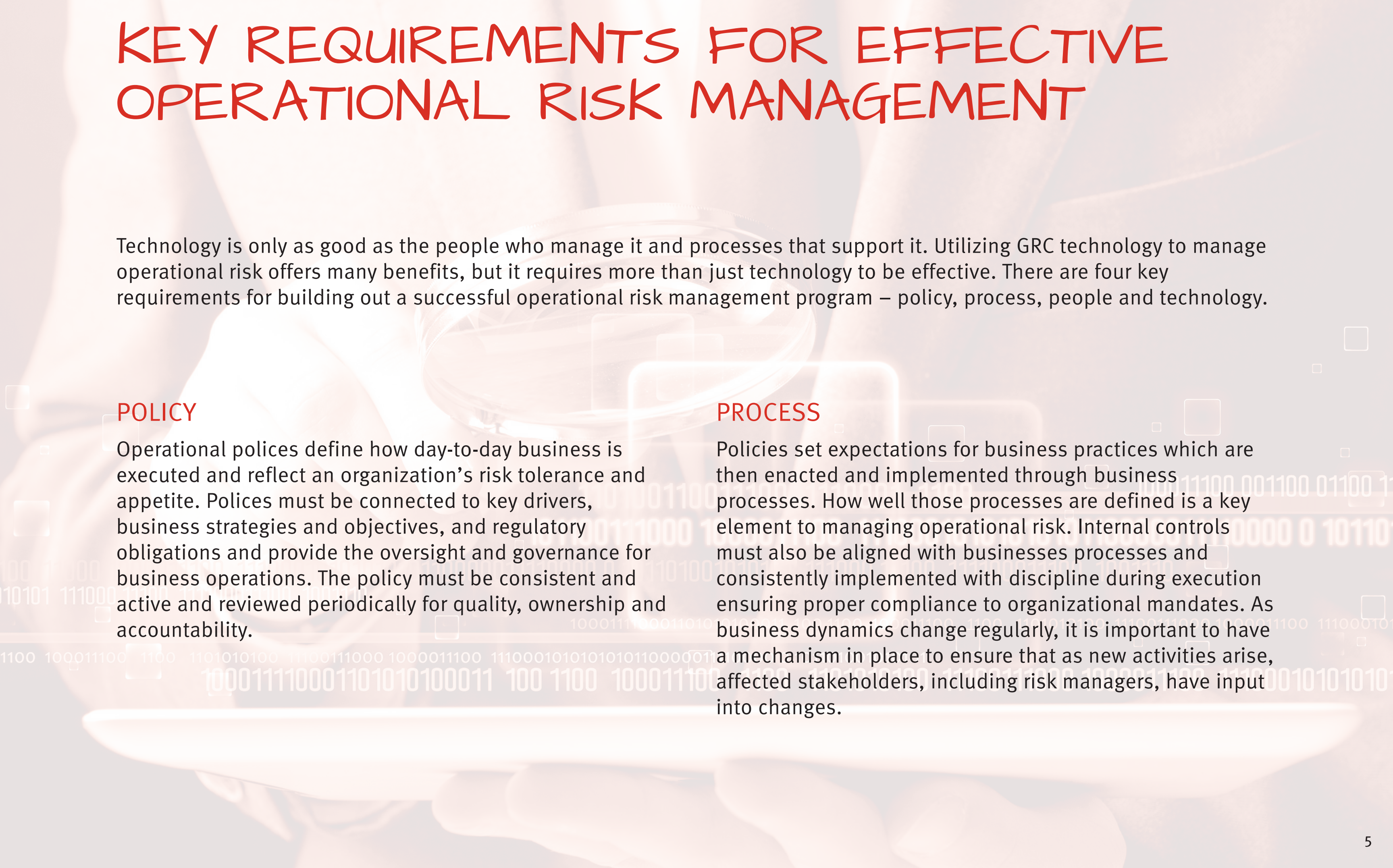


83% of organizations feel the volume and complexity of risks have increased in the last five years.

Source: American Institute of CPAs

[3] NYSE Governance Series, "Managing Cyber Risk: Are Companies Safeguarding Their Assets?" July 2014

KEY REQUIREMENTS FOR EFFECTIVE OPERATIONAL RISK MANAGEMENT



Technology is only as good as the people who manage it and processes that support it. Utilizing GRC technology to manage operational risk offers many benefits, but it requires more than just technology to be effective. There are four key requirements for building out a successful operational risk management program – policy, process, people and technology.

POLICY

Operational polices define how day-to-day business is executed and reflect an organization’s risk tolerance and appetite. Polices must be connected to key drivers, business strategies and objectives, and regulatory obligations and provide the oversight and governance for business operations. The policy must be consistent and active and reviewed periodically for quality, ownership and accountability.

PROCESS

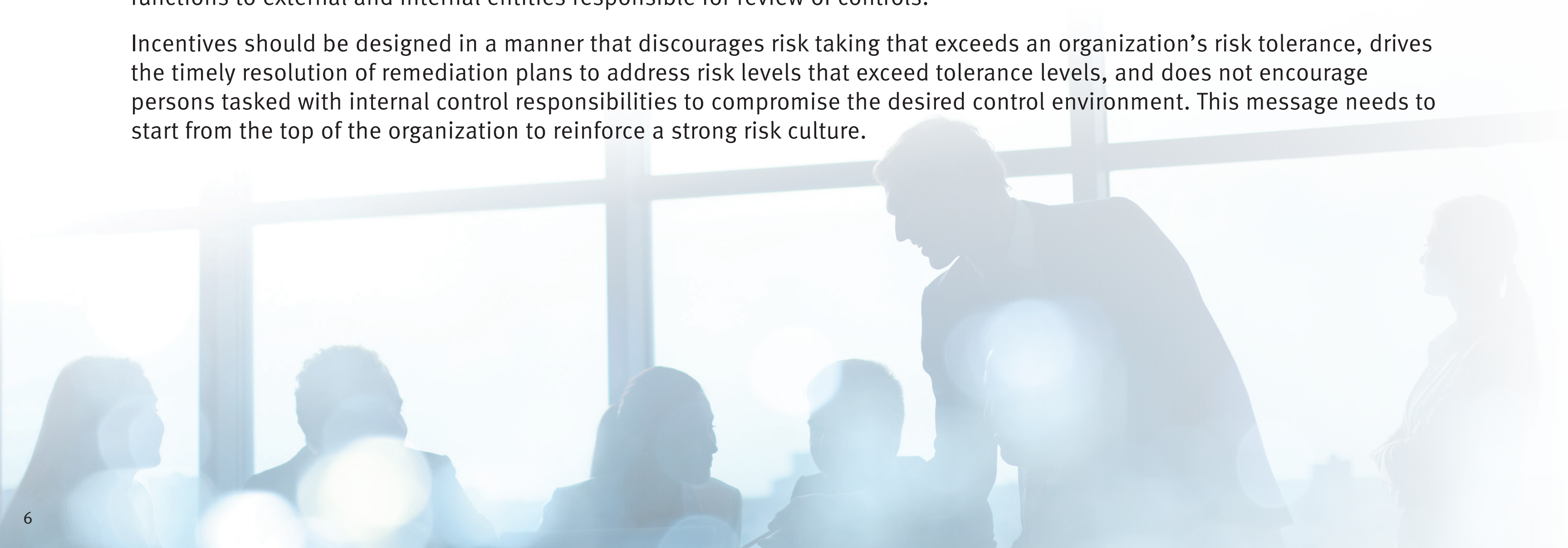
Policies set expectations for business practices which are then enacted and implemented through business processes. How well those processes are defined is a key element to managing operational risk. Internal controls must also be aligned with businesses processes and consistently implemented with discipline during execution ensuring proper compliance to organizational mandates. As business dynamics change regularly, it is important to have a mechanism in place to ensure that as new activities arise, affected stakeholders, including risk managers, have input into changes.

KEY REQUIREMENTS FOR EFFECTIVE OPERATIONAL RISK MANAGEMENT

PEOPLE

Staffing is critical to a successful operational risk management program. Besides ensuring sufficient personnel with relevant experience to manage day-to-day operations, roles and responsibilities and accountability must be clearly defined and understood along the entire chain of risk management – from the front line employees to oversight and management functions to external and internal entities responsible for review of controls.

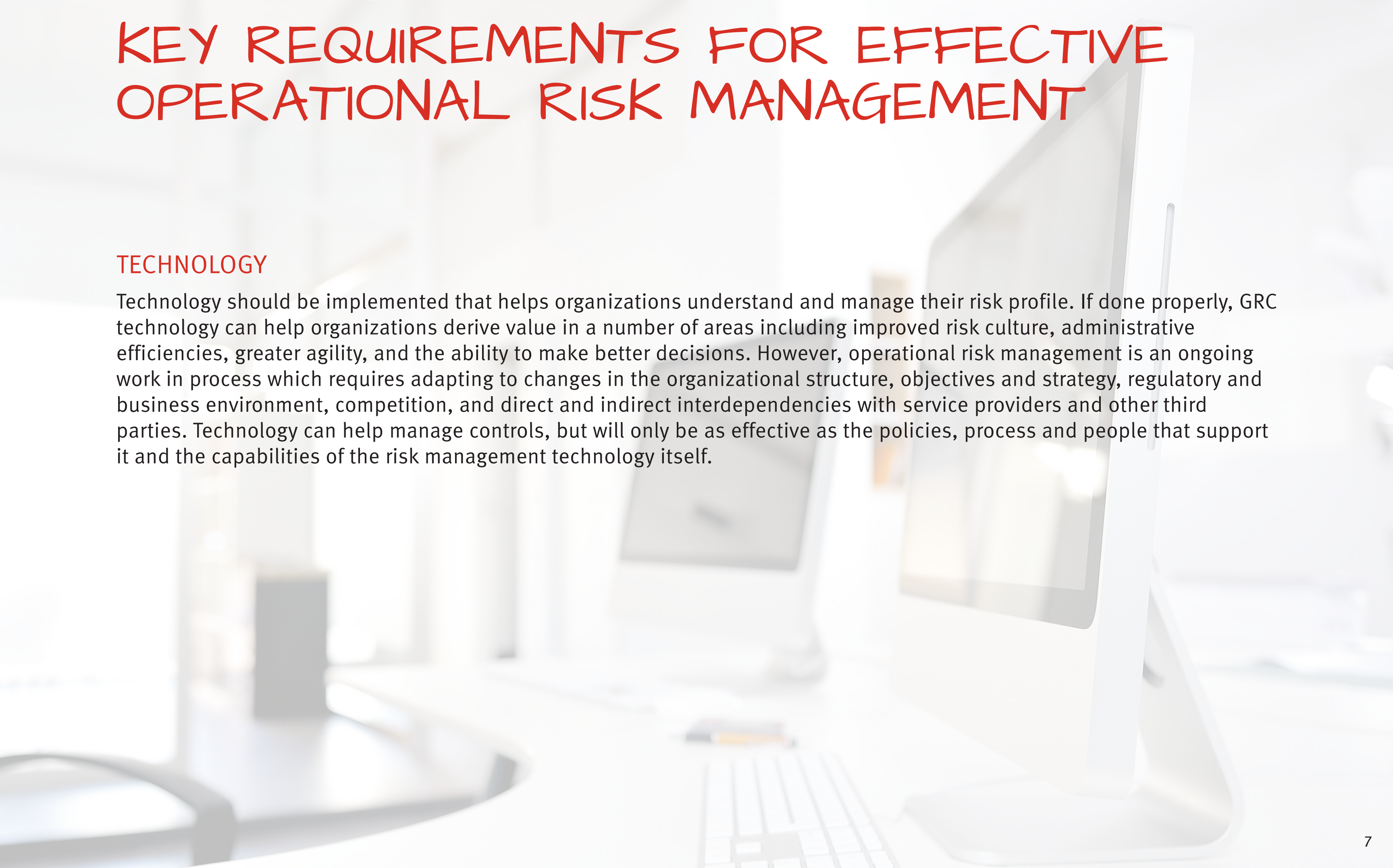
Incentives should be designed in a manner that discourages risk taking that exceeds an organization's risk tolerance, drives the timely resolution of remediation plans to address risk levels that exceed tolerance levels, and does not encourage persons tasked with internal control responsibilities to compromise the desired control environment. This message needs to start from the top of the organization to reinforce a strong risk culture.



KEY REQUIREMENTS FOR EFFECTIVE OPERATIONAL RISK MANAGEMENT

TECHNOLOGY

Technology should be implemented that helps organizations understand and manage their risk profile. If done properly, GRC technology can help organizations derive value in a number of areas including improved risk culture, administrative efficiencies, greater agility, and the ability to make better decisions. However, operational risk management is an ongoing work in process which requires adapting to changes in the organizational structure, objectives and strategy, regulatory and business environment, competition, and direct and indirect interdependencies with service providers and other third parties. Technology can help manage controls, but will only be as effective as the policies, process and people that support it and the capabilities of the risk management technology itself.



CASE STUDIES: GRC IN ACTION

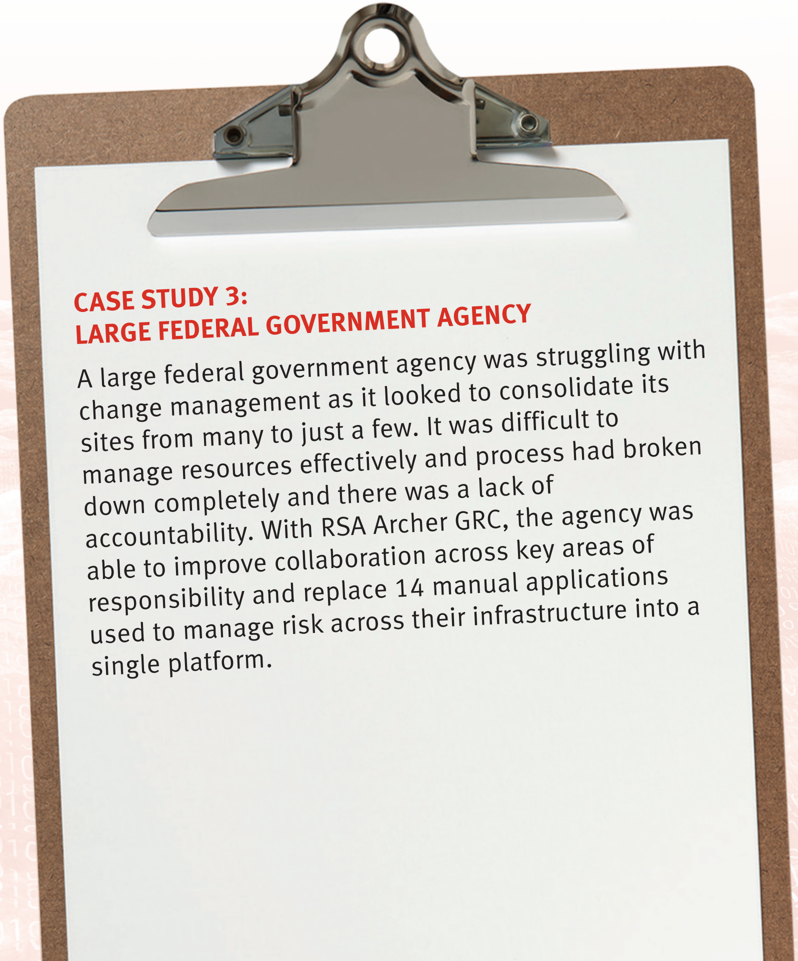
CASE STUDY 1: GLOBAL MANUFACTURING COMPANY

A Fortune 100 global manufacturing company was looking to implement an enterprise-wide GRC program that would provide a comprehensive view of risks across the organization from a single platform. With RSA Archer GRC, the organization was able to build a defined process to compare risks across various functions and business units to enable better decision making and reduce the number of point solutions to be managed.

CASE STUDY 2: FORTUNE 500 FINANCIAL SERVICES PROVIDER

A Fortune 500 financial services provider received designation as a systemically important financial institution (SIFI) which would subject them to enhanced standards and requirements to have an enterprise-wide view of risks across the business. With RSA Archer GRC, the organization has a single view of risk with an enterprise platform that allows stakeholders and business partners to share data, collaborate, and gather the necessary information to make more informed risk decisions.

CASE STUDIES: GRC IN ACTION



CASE STUDY 3: LARGE FEDERAL GOVERNMENT AGENCY

A large federal government agency was struggling with change management as it looked to consolidate its sites from many to just a few. It was difficult to manage resources effectively and process had broken down completely and there was a lack of accountability. With RSA Archer GRC, the agency was able to improve collaboration across key areas of responsibility and replace 14 manual applications used to manage risk across their infrastructure into a single platform.

ABOUT RSA ARCHER GRC FOR OPERATIONAL RISK MANAGEMENT

RSA Archer Operational Risk Management offers an integrated platform to help organizations understand risk across the business. The centralized system provides insight into risk and compliance by company, division, business unit, products and service, business processes, and IT asset. This integrated approach enables analysis of multiple risks across organizational silos and provides actionable insights to help optimize performance within a dynamically changing business climate. As each item can be assigned to an individual, it also enables the accountability and workflow that is so critical to a successful ORM program.

To learn more about RSA Archer Operational Risk Management, please visit https://store.emc.com/rsaarcher.