RSA BUSINESS-DRIVEN SECURITY™

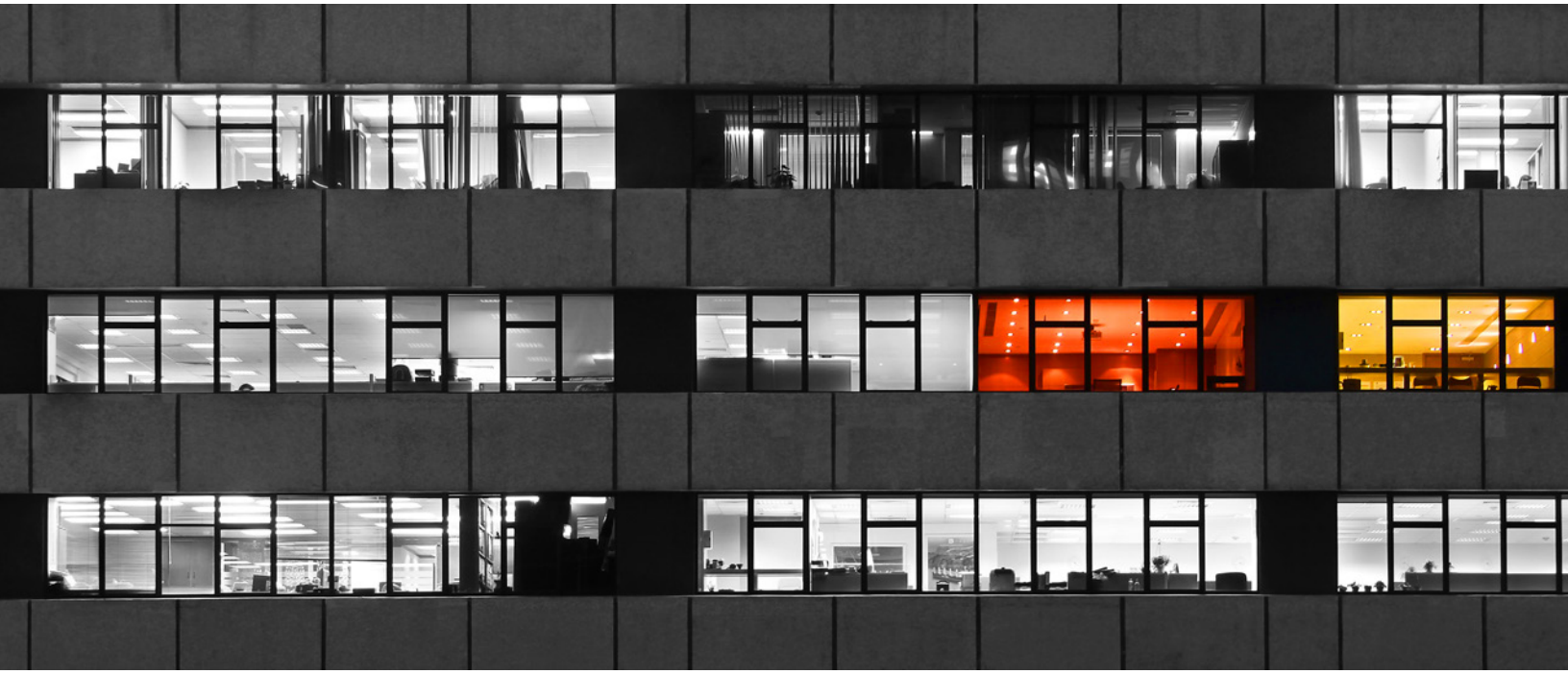
WHITEPAPER

RSA RISK FRAMEWORKS

MAKING DIGITAL RISK MANAGEABLE

RSA BUSINESS-DRIVEN SECURITY™

CONTENTS



EXECUTIVE SUMMARY

Even the most successful companies struggle with understanding their level of maturity in managing digital risk. The forces of modernization, malice and mandates—the rapid digitization of business, growing resourcefulness of malicious actors and increasing regulatory demand placed on businesses—aren't making things any easier. The pressure is increasingly on organizations to effectively and efficiently identify, manage and mitigate these constant challenges.

Modern businesses regularly face high-order challenges, ranging from core cybersecurity functions such as incident management, to digital risks related to privacy, third parties, business resiliency and others. These organizations need to quickly and accurately understand their current capability to mitigate risk, and then create and implement a plan to increase maturity and reduce risk.

To help organizations both assess and address critical categories of digital risk, RSA presents a set of risk maturity models that target specific, high-impact security challenges and risks that increasingly affect all modern organizations. These models, developed through thousands of engagements across some of the most complex business and technology environments available today, are designed to help digitally enabled businesses of all types and sizes assess their current capabilities and plot a path forward.

TRANSFORMING HOW WE THINK ABOUT SECURITY

The forces of modernization, malice and mandates—the rapid digitization of business, growing resourcefulness of malicious actors and increasing regulatory demand placed on businesses—are putting pressure on modern technology-driven organizations to effectively and efficiently identify, manage and mitigate these constant sources of digital risk.

MODERNIZATION

In a transforming world, data is the currency of choice, changing entire industries and offering new opportunities. Data will soon flow freely across workforces, ecosystems and economies—ushering in the era of the modern enterprise. The explosion of information, user preferences, more connected devices, more digital channels to interact with and the realities of managing virtual and hybrid cloud environments also create new security-related complexity.

MALICE

Technological complexity can create an abundance of new opportunities for adversaries, who have more tools, resources and patience than ever before. Increasingly stealthy and virulent malware, costly account takeovers, site-killing distributed denial of service (DDoS) attacks, and persistent ransomware exploiting zero-day vulnerabilities are just a short list of what enterprise security and fraud teams are up against. Despite increasing levels of security spending, we have seen nearly 2,000 data breaches[1] and nearly 2 billion personal records reported stolen[2] in the past two years.

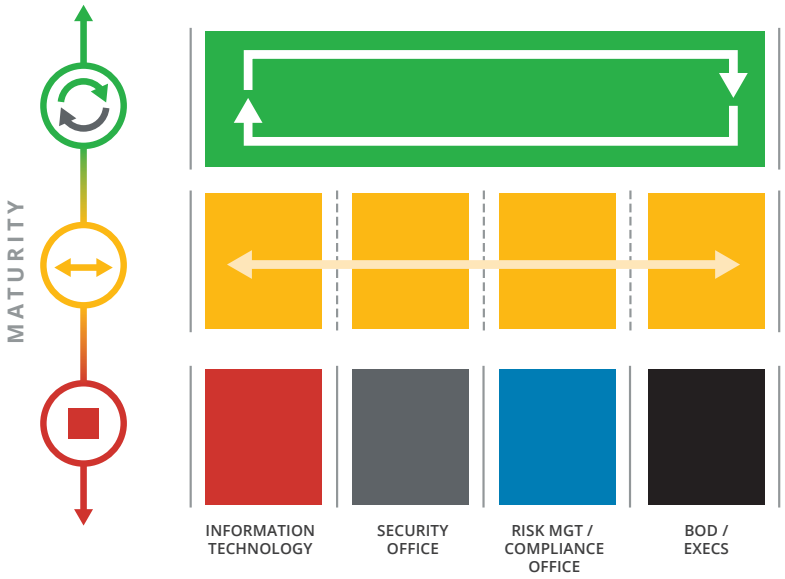
MANDATES

As a result, governing bodies are trying to drive more accountability for data protection and privacy by implementing sweeping regulations. Cybersecurity and data privacy legislation in the UK and elsewhere will radically change how both public and private sectors operate across the interconnected globe. The new General Data Protection Regulation (GDPR) in the EU mandates fines of up to 4 percent of revenue for any global company found in violation of its data-compliance stipulations.

ASSESSING DIGITAL RISK MATURITY

A thorough understanding of current and desired states of maturity is foundational to implementing and measuring the effects of any improvements. Digital risk management is no different.

The RSA Risk Frameworks allow organizations to assess themselves against various industry-standard benchmarks, including the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) version 1.1, to help evolve an organization's digital risk management strategy. By understanding where they stand in relation to such relevant and rigorous industry standards, these organizations can feel confident they are considering and applying best practices, and measuring themselves by the same standards as some of the most complex and critical industries and institutions across the globe.



Digital risk maturity can be measured for any team within the security, risk or IT functions, but generally, the assessment includes the IT, security, and risk management leadership, and the heads of the lines of business and/or the board of directors. The states of digital risk management maturity for these core functions can be broadly grouped into three categories, representing the spectrum of maturity, and with specific characteristics contributing to that general classification:

BASIC

The basic level of maturity is characterized by a largely ad hoc, primarily reactive risk posture. Teams have implemented a limited set of assessments and controls, and few of these systems benefit from automation. The strategy and level of organization is centered on concrete, predictable situations and scenarios, such as static compliance, active threats and others. Organizations at this level of maturity often have not purposefully aligned their security efforts to business priorities or objectives. For many organizations, this is the current state of their digital risk management maturity.

INTEGRATED

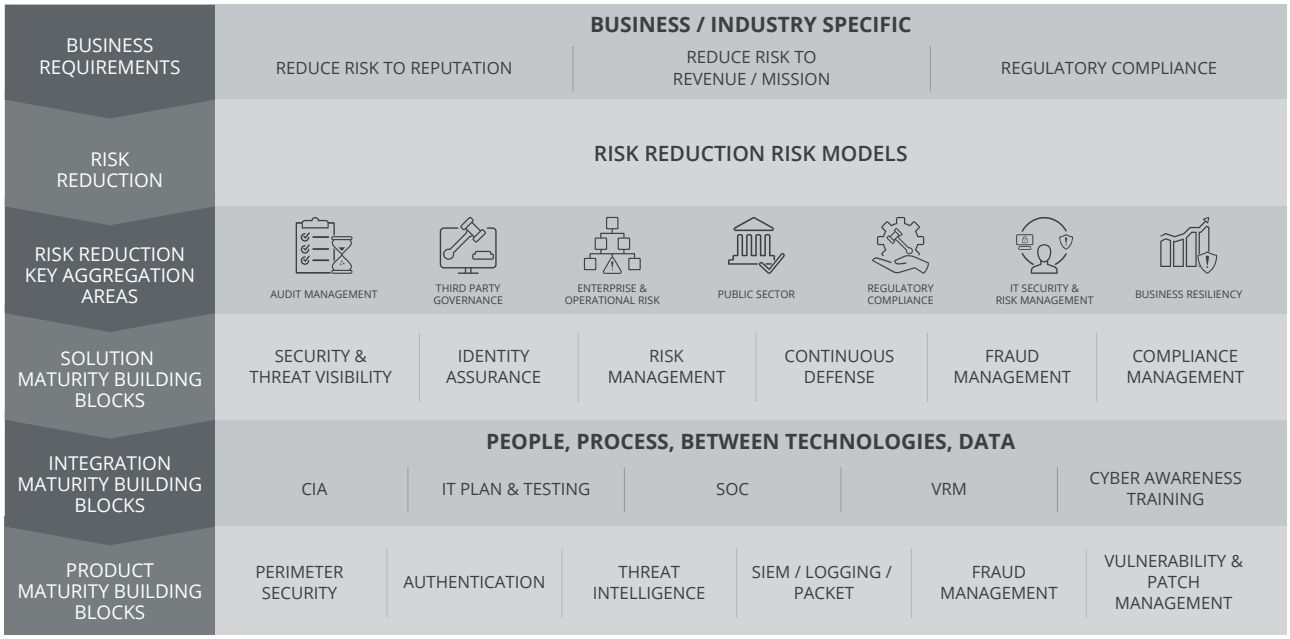
The intermediate level of digital risk maturity is characterized by integration between security and risk teams and the business functions at the heart of the organization's digital risk posture. Businesses occupying this "middle" level of maturity can take a platform approach to use-case solutions, have technology, processes and people in place to solve specific use cases, often solving technical- and threat-oriented needs in a way that does not take into account risk or business context. Teams with integrated maturity profiles benefit from significant improvement and effectiveness over those at a basic level of maturity, but often falling far short of the level of coordination needed to manage multiple levels and sources of digital risk.

OPTIMIZED

The ideal state of digital risk maturity prioritizes business context and operates with a foundational understanding of risk. The optimized digital risk management strategy is characterized by pervasive operationalized visibility, insights gained from that visibility and risk quantification capabilities, and the ability to collaborate and act across and even beyond standard-issue use cases. Organizations working with optimized maturity combine business and risk context to prioritize and align resources and projects with both risk-reducing practices and business objectives. Teams with optimized maturity profiles benefit from significant improvements and effectiveness over those at basic or even integrated maturity levels.

BUSINESS-DRIVEN SECURITY TO REDUCE RISK

Once the organization understands its current level of maturity, that information can be leveraged to create a plan to develop deeper maturity levels in targeted areas, and execute on this plan to reduce risk.



KEY ELEMENTS FOR REDUCING RISK

BUSINESS REQUIREMENTS

The RSA Business-Driven Security risk-reduction model begins with the business requirements for reducing digital risk; for example, many organizations need to reduce risk to reputation, risk to revenue or mission, and risk of regulatory noncompliance.

KEY RISK AGGREGATION AREAS

RSA has identified several critical functions and considerations, such as audit management, third-party governance, enterprise and organizational risk, public sector risk, regulatory compliance, IT security and risk management, and business resiliency.

SOLUTION MATURITY BUILDING BLOCKS

RSA understands that solving digital risk management challenges most often requires a combination of visibility, insight and action. The RSA Business-Driven Security solution sets include identity assurance, continuous defense, fraud management and compliance management.

INTEGRATION MATURITY BUILDING BLOCKS

Within each solution set, RSA standardizes its approach to consider the people, processes, technologies and data that are most critical to implementing the solution, from IT planning and testing to cyber-awareness training.

PRODUCT MATURITY BUILDING BLOCKS

Core capabilities like perimeter security, authentication, threat intelligence, incident detection and management, and vulnerability and patch management make up the overall capability of the risk-reduction solution.

Effective digital risk management reduces risk overall by improving the organization's ability to identify, assess and mitigate digital risk. Implementation of a risk-reduction model helps organizations maximize the value of IT security and risk management investments, and draw deeper value from otherwise disparate point solutions.

DIGITAL RISK FOCUS AREAS

MATURITY IN FOUR KEY AREAS

RSA Risk and Cybersecurity Practice

CYBER INCIDENT RISK MGMT	3RD PARTY RISK	DATA PRIVACY RISK	DIGITAL BUSINESS RESILIENCY
Ability to identify sophisticated attacks & breaches, lateral movement, initial impact and effectively respond with a cross functional response.	Risk is considered from perspective of loss events, opportunity costs and enhancing likelihood of achieving objectives and executing strategy. Risk taking decisions are proactive.	Business context is completely infused into compliance processes and technology. Monitoring capabilities alert stakeholders to impactful regulatory changes.	Integrated information governance into corporate infrastructure and business processes to such an extent that compliance with program requirements and legal, regulatory, and other responsibilities are routine.
Ability to identify commodity malware, some breaches, some lateral movement, basic initial impact and respond with a somewhat coordinated cross functional response.	Management has information needed to understand complete context of risk. More informed decisions made and accountability established but decision process is still manual.	System of record in place to manage full lifecycle of compliance activities. Stakeholders collaboratively define processes and policies; remediation activities are consistently monitored and reported.	Established proactive information governance program with continuous improvement. Information governance issues and considerations routinely integrated into business decisions.
Limited availability to identify commodity malware, some breaches, some lateral movement, basic initial impact and limited ability to respond.	Agreement on risk management terminology, rating scales and assessment approach is established. Little business context is available and responsibility for each risk and control is not always clear.	Operational standards and a comprehensive compliance catalog are developed. Some activity focused on improving effectiveness and stabilize processes with limited scope.	Developing recognition that information governance has impact on organization and benefits from more defined program. Still vulnerable to scrutiny of legal or business requirements.
No ability to detect threats against the organization and no ability to respond when attacked.	Baseline activities are in place to manage risk but are isolated and fragmented. Beginning to obtain visibility into assessed level of inherent and residual risk but accountability is ad hoc	Organization understands broad compliance obligations but each area manages separately. Control performance is assessed ad hoc or as part of external audit.	Information governance and recordkeeping concerns are not addressed at all, minimally or ad hoc. Will not meet legal or regulatory scrutiny or effectively server the business.

Sourced from ARMA International Generally Accepted Recordkeeping Principles

RSA helps customers assess and address critical categories of digital risk, using digital risk maturity models that target specific, high-impact security challenges and risks that increasingly affect all modern organizations, ranging from core cybersecurity functions to digital risks related to privacy, third parties, business resiliency and others.

RSA helps customers apply this idea of advancing stages of maturity cross-functionally to specific challenges that require such an approach. There are four particularly common and challenging areas that require coordination across risk management, security operations and user access for optimal execution.

CURRENT RSA RISK FRAMEWORKS INCLUDE:

CYBER INCIDENT RISK

Designed to help organizations improve their maturity in defending against sophisticated attacks, detecting breaches and applying effective remediation, all aligned with organizational risk objectives.

DATA PRIVACY RISK

Designed to help organizations infuse business context into compliance processes and technology, with monitoring capabilities to alert stakeholders to impactful regulatory changes.

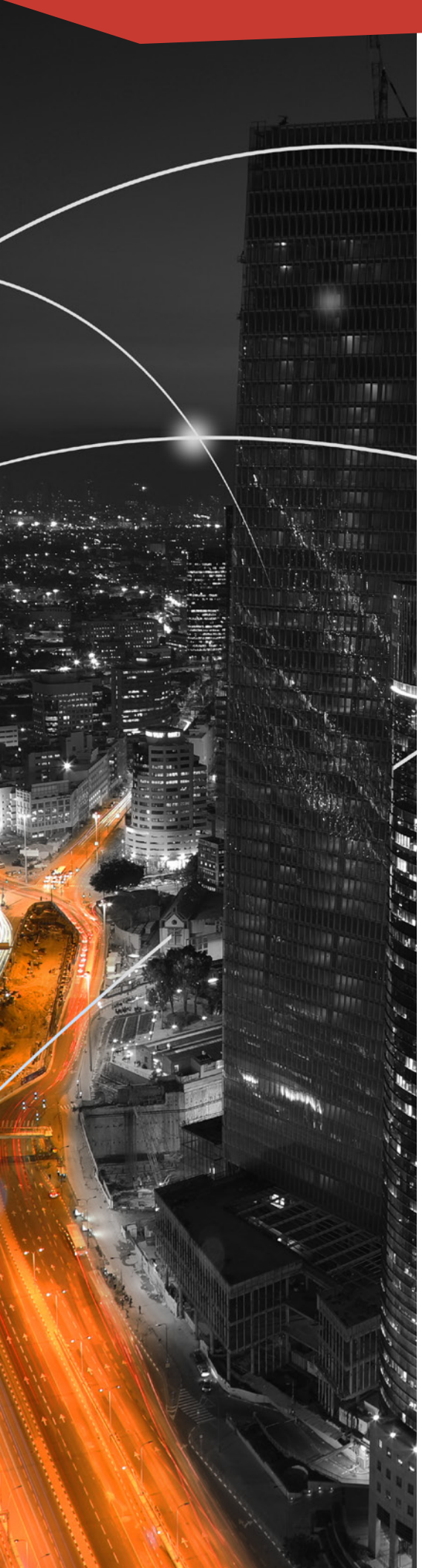
THIRD-PARTY RISK

Designed to help organizations develop a strategy to proactively manage third-party risk around loss events, opportunity costs and potential impacts to achievement of objectives and execution of strategy.

DIGITAL BUSINESS RESILIENCY

Designed to help organizations integrate information governance into corporate infrastructure and business processes so that compliance with program, legal and regulatory requirements are routine.

Each of these challenges needs a common framework for modeling out a state of organizational maturity. The RSA Risk Framework models align with the familiar phases of the NIST Cyber Security Framework (Identify, Protect, Detect, Respond, and Recover) and other standards. Our Risk and Cyber Security Services group can support an assessment of risk posed by the level of maturity across those five phases.



CONCLUSION

As organizations seek to harness rapid technology acceleration, transforming their IT environments and their workforces to better compete in their markets, they must transform their security strategies in parallel.

Migration to include, and increasingly rely upon, cloud, mobile and IoT platforms drastically changes and expands the attack surface. Cyber threats are accelerating, driving far greater risk to organizations than ever before. Moreover, greater risks have led to greater regulatory pressure and demand for continuous compliance. Organizations in this environment require modern, resilient, adaptable and unified security programs to address the new requirements that are evolving from these tranformations.

Improvement starts with assessment, and RSA Risk Frameworks offer organizations a way to understand organizational risk management maturity against foundational industry standards, and plot, execute and measure the effort to achieve greater maturity.

To learn more about how RSA can help your organization better understand and manage digital risk, visit rsa.com.

1. "Verizon Data Breach Investigations Report 2018," Verizon.com, accessed June 21, 2018. http://www.verizonenterprise.com/verizon-insights-lab/dbir/.
2. "Number of compromised data records in selected data breaches as of March 2018 (in millions)," Statista.com, accessed June 22, 2018. https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-world-wide/.

RSA