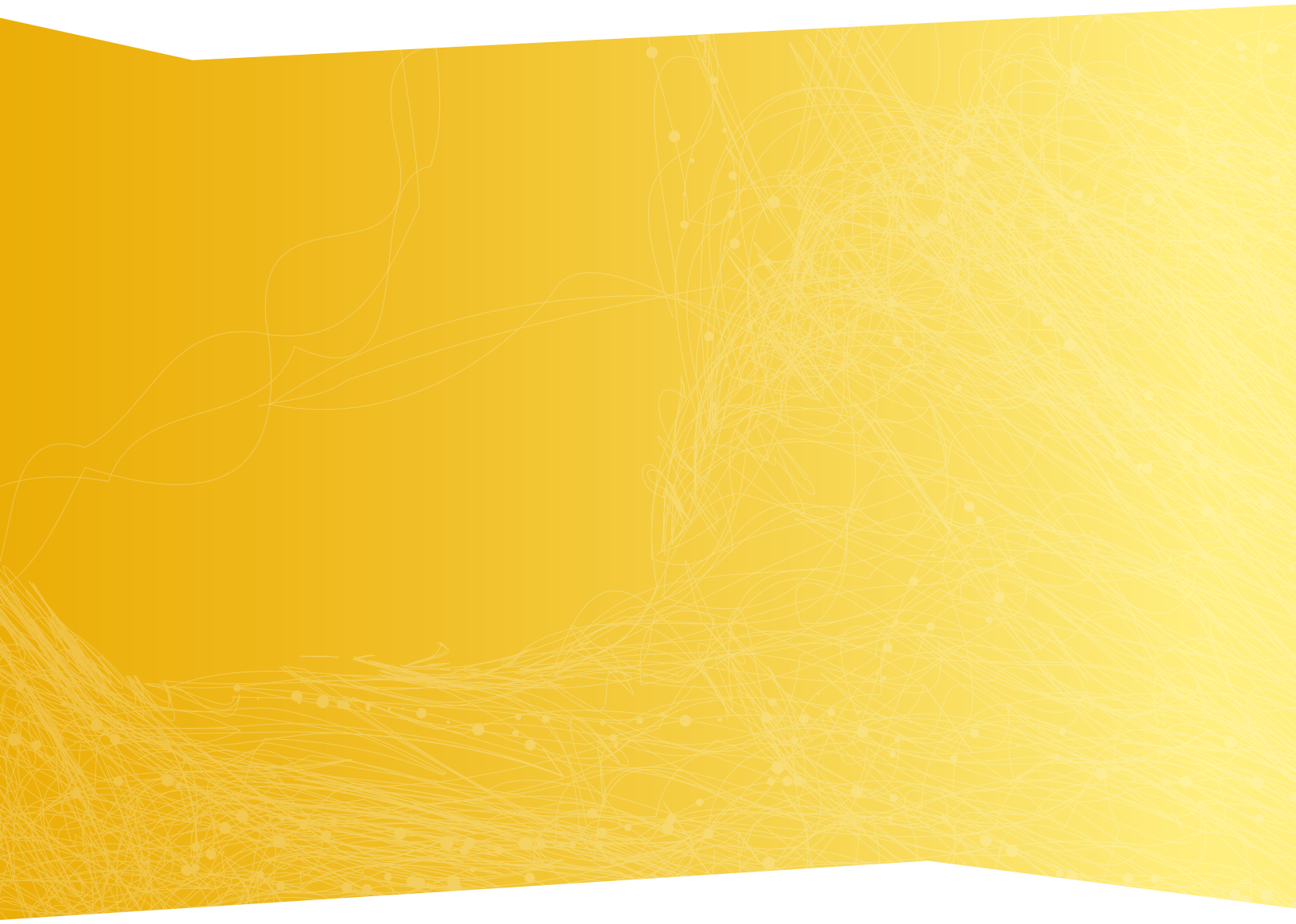
RSA



MATURITY MODEL SNAPSHOT

IT & SECURITY RISK MANAGEMENT

RSA

Another day, another security threat. That's the reality in every organization today. But what's the most effective way to respond? Sure, you can add a new layer of defense for every new threat. But you can only sustain that approach for so long—especially when every layer brings a whole new wave of security data to protect.

As if that weren't enough, there are new challenges looming. With traditional barriers vanishing and external entities playing a larger role, it's tough to see where risks are coming from. It's also easy to lose sight of security's strategic value when every moment is spent fending off immediate threats.

Adding more layers of defenses only adds to the complexity of the problem. It's far more effective to look ahead to ways to mature the organization's IT security processes. That's the way to ultimately reduce the cost of security, increase its effectiveness and make it a strategic enabler of growth.

CAPABILITIES: WHAT IT TAKES TO MATURE IT SECURITY PROCESSES

Managing IT and security risk in this new reality means having a collaborative, coordinated effort to:

- Align security policies with business and regulatory priorities
- Use agile processes to stay ahead of threats and defend against attacks
- Build security strategies that look beyond immediate tactical needs
- Ensure the effectiveness of compliance controls

RSA Archer's IT Security Risk Management solution provides key capabilities to:

Establish a business context for security by ensuring the IT security team understands business and IT assets and relationships.

Lay a foundation of policies and standards on which to build solid IT and security practices and controls.

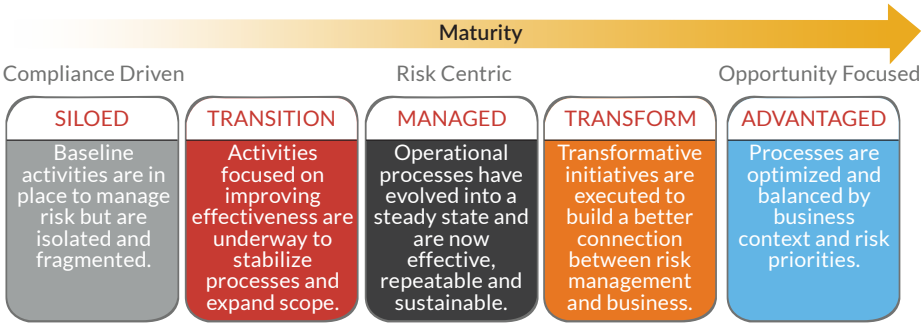
Resolve security and control deficiencies with methods to manage control compliance, threats and vulnerabilities.

Detect and respond to attacks with a solution for day-to-day events as well as serious incidents.

STAGE BY STAGE: MAPPING THE MATURITY JOURNEY

RSA Archer Maturity Models guide organizations through the journey from baseline risk management to optimized processes that balance opportunities and risks. There are five stages along the way:

RSA



THE SILOED STAGE: MASTERING THE BASICS

Organizations at this stage are preparing to evolve traditional approaches to IT security risk management.

- There is minimal knowledge of how IT assets support the business.
- Systems are scanned for vulnerabilities, network data collected in real time, and incident analysis documented—but without a clear business context.

THE TRANSITION STAGE: STABILIZING AND STRENGTHENING

Moving from Siloed to Managed, security teams organize asset information and integrate data sources.

- Processes are developed that align security with business needs.
- Business-relevant regulatory requirements are catalogued and controls established to meet them.
- There is support for security and flexibility to allow log/event/packet analysis beyond critical infrastructure.

THE MANAGED STAGE: STANDING FIRM

The organization gains visibility into security through analytics, effective processes, and efficient metrics.

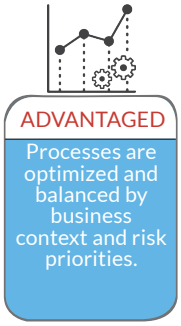
- Both business and technology requirements guide security operations.
- Security issues are reported with both business and IT context.
- Vulnerability-scan data includes business context, and incidents can be prioritized and escalated based on business impact.

THE TRANSFORM STAGE: ASSERTING CONTROL

With better prioritization models, the organization harmonizes across business requirements and reduces overhead.

- A business impact analysis process helps determine asset criticality.
- Both threat and asset information determine criticality of security events.
- Prioritization and triage automatically take into account asset criticality.
- Standardized risk assessments further improve prioritization.

RSA



THE ADVANTAGED STAGE: RIDING THE WAVE

Security speaks the language of business, responding to emerging business requirements with common taxonomies, approaches and decision making processes.

- Business context is completely infused into security processes and technologies.
- The security team reports on issues with integrated business attributes and impact.
- Risk assessment is based on the business profile of the systems and processes.
- Key vulnerability metrics are automatically reported to IT and business stakeholders.
- Data-breach emergency communications extend beyond IT.

Organizations ultimately realize the competitive advantages of harnessing risk: getting to market first, launching new products with calculated efficiency, and avoiding major issues that could wreck reputations and ruin bottom lines.

For more detailed information about the RSA Archer Maturity Model for IT Security Risk Management, visit rsa.com/en-us/resources.

ABOUT THE RSA ARCHER MATURITY MODEL SERIES

RSA Archer's vision is to help organizations transform compliance, manage risk and exploit opportunity with Risk Intelligence made possible via an integrated, coordinated GRC program. The RSA Archer Maturity Model series outlines the segments of risk management that organizations must address to transform GRC.

ABOUT RSA

RSA offers Business-Driven Security™ solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high risk world.
For more information, visit rsa.com.

Copyright ©2017 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA 5/17, Maturity Model Snapshot H16148

Dell Inc. or its subsidiaries believe the information in this document is accurate as of its publication date. The information is subject to change without notice.