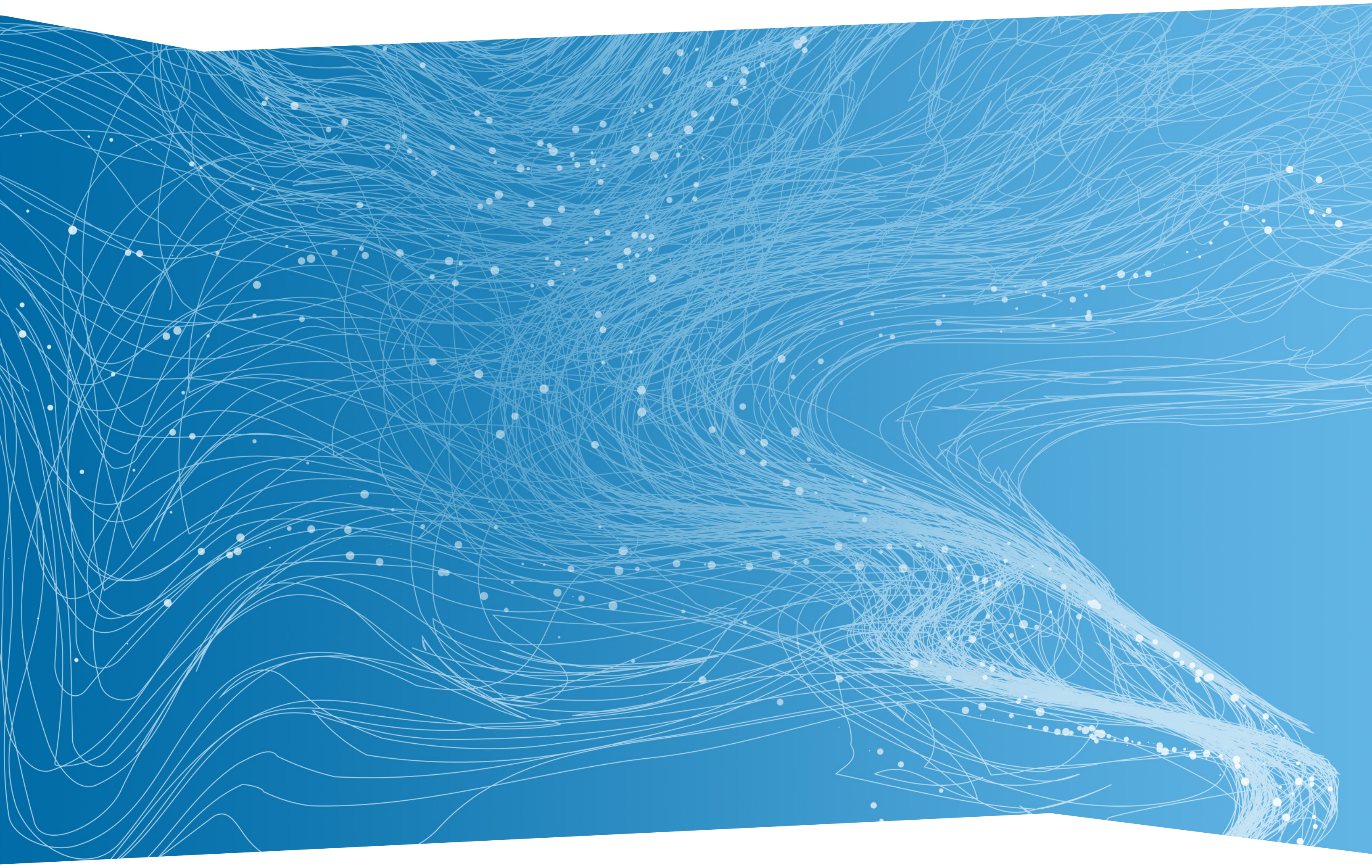


WHITE PAPER

RSA ARCHER® MATURITY MODEL: OPERATIONAL RISK MANAGEMENT

WHITE PAPER

RSA

OVERVIEW

Effectively managing risk has become a matter of competitive advantage and, sometimes, business survival. Organizations face an increasingly challenging landscape where the number, complexity and velocity of operational risks are continually mounting. The RSA Archer Maturity Model for Operational Risk Management outlines RSA Archer's role in the critical stages in a company's journey from reactive, compliance driven processes to a risk-centric, opportunity-focused operational risk program that provides competitive advantage to fuel the enterprise.

CONTENT

Why Operational Risk Management? 1

Key Capabilities 1

The Maturity Journey 2

Maturity Model Crossover 8

Conclusion 9

About RSA Archer Maturity Models 10

RSA

WHY OPERATIONAL RISK MANAGEMENT?

Managing risk today has become a matter of business survival. Organizations face an increasingly challenging landscape where the number, complexity and velocity of operational risks are mounting. The speed at which these risks are emerging means organizations have a much less time to effectively respond. Slow response can have a devastating affect and could even shutter a business entirely. Business managers and their teams are overwhelmed with the increasing risk-related workload and, as a result, are either not always fully aware of high risks or cannot get in front of these issues to adequately manage them. Teams often struggle with identifying business priorities and assigning accountability to known risks. This leaves business line managers and risk management teams scrambling to react when risk incidents occur.

Unfortunately, many organizations do not take a proactive, comprehensive approach to managing risk. Instead, they manage many different types of risks (like cyber, third party supplier, competitive and new product/service risks) within different business silos and assess those risks using separate methodologies and measurements. This makes it very difficult to provide management with an accurate and aggregated view of risk across the business. Without clear visibility, risk cannot be consistently managed within the organization's risk appetite.

The executive team and Board of Directors must have confidence that they have a complete understanding of the organization's risk profile in order to make good business decisions and fulfill their fiduciary obligation. In addition, they need assurance that the organization's internal control framework is adequately designed and operating to insure that risk is being effectively managed. Operational risk management strives to bring together this picture of operational risk, raising the visibility of issues and providing the critical input necessary to make more effective and calculated decisions that increase the likelihood of achieving objectives or reducing the frequency and impact of adverse events.

KEY CAPABILITIES

An operational risk management program brings together data from fragmented risk repositories to identify, assess, decision, treat and monitor risks consistently across the organization. For most companies, their current approach to operational risk management overwhelms resources, does not provide a consistent, real-time risk picture to the executive team, and does not effectively and efficiently engage each of the three lines of defense (business units, risk managers, and audit). By consolidating risk information into a central repository and measuring and treating risk in a consistent fashion, risk functions can quickly obtain an accurate picture of risk for the Board and executive team.

RSA Archer GRC Maturity Models focus on key capabilities enabled by the RSA Archer solution. As a technology enabler, RSA Archer provides the critical infrastructure to leverage processes, share data and establish common taxonomies and methodologies.

RSA Archer serves as a central aggregation, visualization, and governance point for the organization's operational risk management program. RSA Archer enables risk functions to better understand risk, prioritize and manage risk, and reinforce desired risk management accountabilities and culture. This allows operational risk management programs to extend across all business lines and activities that introduce operational risk. With RSA Archer Operational Risk Management, the organization can harness risk intelligence to reduce the likelihood of negative events, lost opportunities, and surprises, enabling the business to maximize performance.

To achieve these goals, RSA Archer's Operational Risk Management solution focuses on the following key capabilities:

Establish scope and context for operational risk management
Enabling the risk function to understand the business and IT assets, relationships and criticality, establish ownership and accountability and lay the foundation for operational risk reporting.

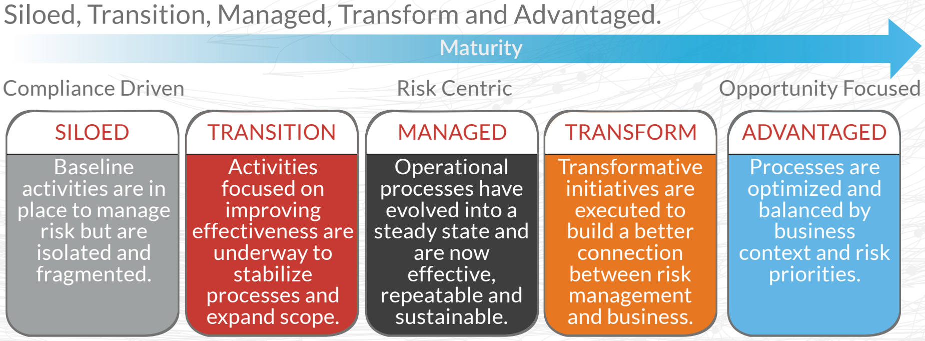
Identify and assess operational risks
Processes to identify existing and emerging risks, capture and analyze loss events, establish key metrics and indicators, and capturing changes to the business to assess risk.

Decision and treat operational risks
Efficient methods evaluate inherent and residual risk levels and establish risk treatments through policies, standards and controls

Report on and monitor operational risks
Processes to provide accurate and timely reports to management, risk and control owners and other stakeholders and ensure the risk management framework is administered and managed.

THE MATURITY JOURNEY

RSA Archer Maturity Models are segmented into five major stages: Siloed, Transition, Managed, Transform and Advantaged.



SILOED	TRANSITION	MANAGED	TRANSFORM	ADVANTAGED
Baseline activities are in place to manage risk but are isolated and fragmented.	Activities focused on improving effectiveness are underway to stabilize processes and expand scope.	Operational processes have evolved into a steady state and are now effective, repeatable and sustainable.	Transformative initiatives are executed to build a better connection between risk management and business.	Processes are optimized and balanced by business context and risk priorities.

The RSA Archer Maturity Model is designed to be pragmatic and implementable. Elimination of the "Level 0" that typical Maturity Models include to avoid the unnecessary definition of a stage of maturity that will not meet today's operational risk challenges.

- The **Siloed stage** focuses on baseline activities that all organizations need to manage risk.
- The **Managed stage** is intended to depict the phase that organizations reach a coordinated, sustainable operational risk program.
- The **Transition stage** and **Transform stage** help the organization "move to the next level" with initiatives that evolve critical capabilities, setting the stage for advanced capabilities.
- The **Advantaged stage** is designed to be achievable for most organizations, allowing the organization to target an advanced stage of maturity that characterizes an optimized operational risk management program.

The RSA Archer Maturity Model for Operational Risk Management focuses on building these capabilities over time, implementing the broad strategy with tactical, intelligently designed processes.

FOUNDATIONS

Foundations are critical elements necessary for the overall success of the Maturity Journey. Without these foundations in place, the organization will face difficulties throughout the journey either through the lack of focus, commitment, resources or strategy. Any organization looking to improve their operational risk maturity should discuss and address these foundations. Without a strong foundation, organizations may not be successful implementing their operational risk management program. Foundational elements include.

- **Management commitment –** The degree and level of leadership commitment to operational risk management culture, strategy and priorities should be established as maturing risk processes takes time and resources.
- **Performance and acceptable risk -** Defined levels of performance and acceptable risk for operational risk need to be established to set the target state for the risk program and ensure the business understands the level of risks involved.
- **Expectations and measurement -** Clear expectations and success criteria defined for the operational risk management program must be communicated by management to guide strategies.
- **Stakeholder involvement –** Key business stakeholders and constituents need to agree on the importance of continuous improvement and maturity of operational risk processes.
- **Budget and resources –** Sufficient resources for the operational risk management program must be committed to achieve success.

SILOED

Baseline activities are in place to manage risk but are isolated and fragmented.

THE SILOED STAGE: IMPLEMENTING THE BASICS

In the Siloed stage, In the Siloed stage, the organization has a partial inventory of its people, processes, and technology. Inventories reside in different locations, in different formats and may be maintained using different technologies. In some cases, there are multiple overlapping inventories without any one system of record. Inventories that typically exist at this stage include physical facilities, software applications, organizational structure (such as depicted through the organization's accounting system) and a listing of human resources.

Various managers and internal audit have identified and assessed risks in parts of the organization but there is not yet a robust formal approach to methodically identify risks across the organization or to assess the risks in a consistent manner. Loss events are captured in the general ledger by amount, type, circumstance and impacted business unit, but nothing much is being done with the loss events to understand how they relate to risks, controls and risk transfer.

Control procedures have been identified and documented for at least part of the organization. A central repository of controls exists and may be maintained by the internal audit team. The organization's policies and procedures are documented in one location, as are its insurance policies.

The organization is beginning to obtain visibility into assessed levels of inherent and residual risk but accountability for risk and how it is to be decisioned is ad hoc. The organization is able to produce a list of known risks and controls, but the source of information for the list may be spread out in different areas of the organization and in different formats. Information about risks and controls is inconsistent and often incomplete. In fact, the most complete list of risks and controls may be maintained not by management but by the internal audit team.

TRANSITION

Activities focused on improving effectiveness are underway to stabilize processes and expand scope.

THE TRANSITION STAGE: BUILDING CONTEXT FOR THE FUTURE

When an organization is in the Transition stage, more infrastructure is cataloged and associations between infrastructure elements begin to be documented. Included in the Transition phase is cataloging products and services and IT systems and greater detail about the organization's structure, which begin to be mapped together.

Agreement on risk management terminology, rating scales and assessment approach is established and applied consistently across the organization, along with the adoption of the "three lines of defense" concept. Higher level risk statements are created and mapped to the risk register, and risk assessments are performed exclusively in qualitative terms. In addition to actual losses, the organization begins to capture near misses and external loss events and catalogs all outstanding internal and external audit issues, regulatory examination findings and remediation plans in one central location.

By mapping the risk register to the control register and control procedures to policy and procedures and regulatory obligations, the organization is beginning to have an understanding of its risk profile. Coupled with formal documentation about acceptable levels of risk and authorities delegated to named individuals to accept risk, management is making risk decisions but often without complete understanding of the business context of risk.

Sufficient progress has been made in cataloging and assessing risks and controls that a list of key risks and controls can now be generated. While this represents consistent terminology and assessment rating scales, very little business context is available and responsibility for each risk and control is not always clear.

MANAGED

Operational processes have evolved into a steady state and are now effective, repeatable and sustainable.

THE MANAGED STAGE: OPERATIONALLY SOUND

In the Managed stage, the majority of infrastructure elements have been documented in central repositories, with little or no redundancies and overlap. Business processes, IT network devices, third party relationships, regulatory obligations and organizational business units are cataloged. Accountability is established by cross-mapping human resources, organizational structure, business infrastructure, IT infrastructure, third party relationships and regulatory obligations.

With an organization-wide commitment, the first line of defense identifies their risks, performs self-assessments of inherent and residual risk, and documents controls and assets to the control's operation. The second line of defense challenges self assessments of inherent and residual risk, and documents controls and assets to the control's operation. The second line of defense challenges self-assessments for accuracy and completeness. As an output of these assessments, accountability for all identified risks and controls are associated with business units and named individuals.

As loss events are captured, they are mapped to the associated risk register record and can be reported on. Root cause analysis performed to minimize the likelihood of similar losses occurring in the future. Very impactful and volatile risks may be assessed in monetary terms to provide a better understanding of the organization's exposure, rather than what is represented using typical qualitative risk assessment scales. Monetary risk assessments facilitate more meaningful discussions of the adequacy of the organization's insurance risk transfer.

With the interconnection of business infrastructure information to IT infrastructure, business obligations, business hierarchy, human resources, third parties, risks and risk treatments, and policies and procedures, management has the information needed to understand the complete context of risk. This provides for more informed risk decisions and establishes necessary accountability for effective management of risk. However, the decision process is still largely manual and the existence and operation of control procedures is largely based on management assertion.

Each stakeholder is regularly provided with a list of their risks and controls that depict risk consistently on an inherent and residual basis so that they can understand the level of risk relative to risk tolerance. Stakeholders also receive regular reports of loss events and outstanding issues and remediation plans. With this information, senior management and the Board are able to understand who is accountable for risks, controls and loss events and whether loss events are trending in the wrong direction or being effectively managed. They are also able to determine whether identified issues are being addressed by accountable individuals in a timely manner. Notifications are automatically generated to stakeholders to assist them in monitoring issues and remediation plans coming due and those that are past due, as well as when residual risk levels fall outside established boundaries. The second line of defense has the necessary reports to oversee day to day administrative functions, such as the status of risk assessment campaigns in-process, loss events that have not been subject to root-cause analysis and approval, and missing or adversely trending key indicators.

TRANSFORM

Transformative initiatives are executed to build a better connection between risk management and business.

THE TRANSFORM STAGE: PRIORITIZATION AND CONTROL

Business objectives and strategies are clearly established and documented as the organization's focus becomes more proactive. A complete picture of the interrelationship of IT infrastructure is established, mapping software applications to the systems that support them, databases that store the information, and the networking infrastructure that supports the organization.

The Transform stage of risk identification and assessment is marked by greater understanding of the business context and drivers of risk. Risk assessments begin to target business processes, with identified risks explicitly mapped to the business process. Loss events are critically analyzed to understand trends and to determine the root cause and remediation actions for large losses in order to minimize similar future occurrences. Key risk, performance and control indicators are identified and mapped to business units, and named individuals and changes in business activities, infrastructure and regulatory obligations are captured and assessed to understand the impact of the changes on the risk profile.

Risk decision processes are automated. The acceptance of risk by managers within their delegated authorities is enforced through technology, and risk decisions that exceed delegated authority are automatically escalated.

In addition to management's assertion about the design and effectiveness of control procedures, management and audit tests of control procedures are captured along with results of continuous control monitoring tools. This information is reflected in the organization's risk profile on an ongoing basis, and deficiencies in risk treatment, including insurance risk transfer, are actively managed.

Risk reports are provided that depict the roll-up of risk from a granular business unit level to an enterprise risk statement. With the mapping of the organization's business and IT infrastructure, obligations, human resources, third party relationships, risks and risk treatment, risk can be examined and monitored from a broader perspective. This includes risk by product and service, business process, facility, software application, IT system, database and device, third party relationship, risk type and regulatory obligation.

Monitoring of key indicators provides early warning of changes in risk profile. Insurance policies are monitored and re-evaluated on a regular basis to affirm their appropriateness, and notifications to stakeholders are automatically generated when large loss events are recorded or key indicators fall outside of boundaries. This enables stakeholders to respond quickly to losses and changing risk.

The second line of defense has confidence that operational risk management information is accurate and complete because their risk management information system is adequately designed to enforce data integrity.

ADVANTAGED

Processes are optimized and balanced by business context and risk priorities.

THE ADVANTAGED STAGE: OPTIMIZED FOR RISK MANAGEMENT

In the Advantaged stage, the mapping of all infrastructure elements is complete. There is a clear understanding of the "ownership" of strategies and objectives; the products and processes that support the strategies and objectives; the business processes that exist to enable the products and services and strategies and objectives; the IT infrastructure that supports each of the business processes; and the regulatory obligations with which the organization must legally comply. Accountability by named individual and business unit is core to a sound operational risk management program, reinforcing the desired risk management culture.

In the Advantaged stage, risk is considered not just from the perspective of loss events but also as opportunity costs and enhancing the likelihood of achieving objectives and executing strategy. Approaches to risk identification and risk assessment are proactive, forward looking and all inclusive. This includes employment of scenario analysis to identify low frequency, high impact events; factoring scenarios, loss events and metrics into risk assessments; capturing and assessing the risk of all sources of change prior to implementation; utilizing leading performance and risk indicators wherever possible; and enabling automated calculations of risk levels as changes in risk drivers occur.

Risk taking decisions are proactive. Prospective changes in strategy and objectives, products and services, people, process, technology and business obligations are captured automatically, routed to stakeholders for evaluation using consistent risk assessment terminology and techniques, and decisioned within the organization's appetite for risk.

Control deficiencies identified in any manner including loss events, incidents, self-assessments and scenario analysis are addressed, but decisions regarding risk treatment account for the cost to mitigate and transfer risk relative to the amount of risk reduction that the risk treatment provides.

Risk reporting and monitoring is most robust. Stakeholders receive regular reports of risk to strategy, objective and regulatory obligation. Changes that affect risk profile are reported from wherever they originate within the organization, as are reports that monitor all approved risk-related policy exceptions.

Operational risk information is delivered in a variety of ways, including dashboards, push technology and on-demand and ad-hoc requests. In each case, stakeholders can dynamically drill into reports to traverse all inter-related records to understand the business context and drivers of risk.

The second line of defense can easily configure the organization's risk management information system to tailor taxonomy, assessment methodology, workflow and reporting to the unique requirements of the organization and to make modifications as the organization grows.

MATURITY MODEL CROSSOVER

Operational risk – errors and fraud associated with people, processes, technology and external events – covers a very wide range of risks. It is closely related to the other RSA Archer Maturity Models in this series, including Regulatory and Corporate Compliance Management, IT Security Risk Management, Business Resiliency, and Third Party Governance.

For example, IT security risk is cited by executives as one of the fastest growing areas of risk today and holds a significant place in an organization's strategic portfolio of risks. Therefore, IT security risk management should be factored into an organization's operational risk program. Business resiliency is another major issue, given that operational incidents can quickly escalate into a major crisis. Companies can address this by ensuring crisis management, disaster recovery and business continuity planning processes are aligned with operational risk management strategies. Third party governance must be included in operational risk management given many organizations rely heavily on external parties for critical business operations.

Finally, compliance risks are constantly changing in today's regulatory environment and can lead to significant regulatory fines, reputational damage and compliance issues. Regulatory and corporate compliance management is necessary to ensure controls are aligned with compliance obligations as well as risk management requirements.

CONCLUSION

Having a mature operational risk management program in place is essential in transforming risk to an advantage position that enables the business to exploit opportunities. To achieve this level of maturity, companies in the Siloed stage must align priorities and resources across functions to start building a more fluid approach to identifying and treating operational risk. With this alignment, the organization can begin to gain insight and visibility into the business to adjust strategies and break down the risk silos.

In order to move from the Siloed stage to Managed, organizations Transition through projects to catalog and organize asset information and formalize risk practices. Companies in the Managed stage have established a common taxonomy and "language" of risk so that individual silos can share information and processes. As this integration improves, the organization can start getting ahead of the curve on major risk issues. The organization has common data and analytical capabilities, effective risk assessment processes and efficient methods to measure, monitor and report on risks activities.

To reach the Advantaged stage, risk processes Transform by focusing on understanding business context and drivers of risk to rationalize controls and strategies, which harmonizes across business requirements and reduces administrative overhead and costs. The organization can now manage the full risk lifecycle – risk identification, assessment, decision, treatment and monitoring -- and processes for risk are well established and can keep up to speed with the business. This allows executives to make risk-based decisions to shape business strategies and ensure the organization is prepared for emerging risks or events.

Organizations in the Advantaged stage are ready to realize the competitive advantage of harnessing risk, such as beating competitors to market, launching new products and services with calculated efficiencies, and avoiding major issues that affect reputation and the bottom line. Using common taxonomies, common assessment approaches and well-oiled decision making processes, risk and business functions in this final phase speak a common language and have built a culture that can identify and respond to emerging business requirements ahead of the curve.

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 of white papers outlines multiple segments of risk management that organizations must address to transform their GRC programs.

ABOUT RSA

RSA's Intelligence Driven Security solutions help organizations reduce the risks of operating in a digital world. Through visibility, analysis, and action, RSA solutions give customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, prevent IP theft, fraud and cybercrime. For more information on RSA, please visit rsa.com.

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.