RSA® RISK AND CYBERSECURITY PRACTICE

Enabling business driven security

EXECUTIVE SUMMARY

Business Driven Security

The RSA Risk and Cybersecurity Practice provides a portfolio of services that enables organizations to reduce risk by aligning security programs with business objectives. The agility and cost efficiencies associated with cloud, mobile and IOT are delivering on the business promises of efficiency and effectiveness in IT operations. These trends, and the demands of regulatory compliance need to be balanced with adequate controls and safeguards to ensure that the overall propensity for risk is being adhered to.

Organizations seeking to identify gaps, improve readiness, evaluate risk, meet compliance and rapidly respond to incidents can avail of services from RSA's Risk and Cybersecurity Practice, which specializes in tackling such complex challenges.

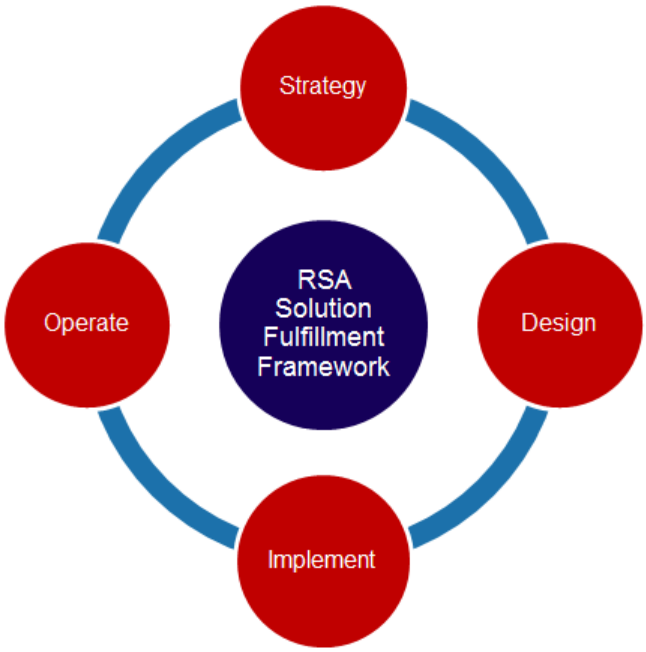
METHODOLOGY AND APPROACH

A holistic framework for end-to-end solution fulfillment

RSA addresses the lifecycle of solution fulfillment, from Strategy & Design to Deployment & Operations Management. The combination of technology and advisory expertise enables RSA to develop a holistic assessment of cybersecurity needs, reduce risk and rapidly respond to incidents.

Additionally RSA provides a range of consulting services to address the "people, policy and process" aspects of a security program.

RSA's professional services teams help customers to optimize their investments in platforms such as the RSA NetWitness Suite, the RSA Archer Platform and the RSA SecurID Suite, amongst others. When combined with our technical expertise, RSA can fulfill end-to-end security and risk management program requirements, within a holistic an integrated Solution Fulfillment Framework.



RSA Solution Fulfillment Framework

Services portfolio ranging from requirements analysis and solution design to deployment and go-forward solution management

RSA Risk and Cybersecurity Practice is aligned across key customer requirement areas:

- RSA Risk Management Practice
- RSA Incident Response Practice
- RSA Advanced Cyber Defense Practice

RSA RISK MANAGEMENT PRACTICE

Enterprise program development

Risk management programs empower organizations to efficiently implement risk management processes to significantly improve their business risk management maturity. RSA Risk Management practitioners provide industry expertise and best practices to design proven, multi-disciplinary risk management solutions in the most efficient manner. Enterprise Risk Management services leverage the RSA Archer Platform and include:

- *RSA Archer Platform Strategy & Roadmap* - designed to identify the elements required for the foundation of a holistic risk management program, targeting early wins while also developing longer term strategy.
- *RSA Archer Platform Optimization Assessment* - business management stakeholders are engaged to design and develop solutions for specific risk and compliance requirements.

Preliminary Use-Case List

		Discovery Session Use-Cases
Laws & Regulations	Interpretation Applicability Business Process Mapping	Regulatory Sourcing Regulatory Review / Applicability Regulatory Mapping Regulatory Change Roll-Out
Change Management	Impact Analysis Gaps Implementation	Change Management Sourcing Enterprise Compliance Impact Analysis Business Unit Implementation Plan Compliance Liaison Reporting
Control Library	Business Self Assessment System Control Process Controls FOPPs	Controls Catalog Generation Controls Classification Controls Mapping FOPP, SOP, Desk Guide Decomposition
Risk Assessment	Regulatory Risk Assessment Inherent and Residual	Risk Categorization Risk Register Regulatory Risk Assessments Risk Appetite Program Tie-In
Testing & Monitoring	Validation of Processes Transaction Testing Sampling	Control Scoping Control Testing (Attribute / Workpaper) Compliance Reporting Continuous Controls Monitoring Validati

RSA Enterprise Risk Management Program Strategy

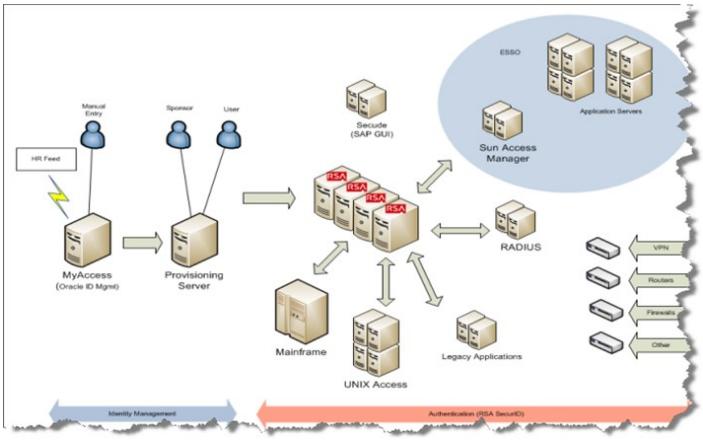
Findings Report with use cases designed to align the security program with business requirements. The rollout plan targets near and medium term RSA Archer Platform solution deployment priorities

RSA IDENTITY ASSURANCE PRACTICE

Enterprise identity management

Identity is the core of all security programs and represents the most consequential threat vector. RSA identity consultants can help with the most complex governance, lifecycle and multi-factor authentication challenges and also help to define and plan your identity and fraud programs to reduce the risk of tomorrow's threats. RSA has been working with customers for over thirty years as a leading provider of identity assurance solutions. Services include:

- *RSA Identity Assurance Strategy* - critical assets, privileged users and users with higher exposure levels (e.g. remote users and partners) are reviewed to align control requirements with risk propensity levels. Systems reviewed include Identity & Access Management, Enterprise Resource Planning, Customer Resource Management, Enterprise Content Management and technologies such as PKI, TLS, RADIUS, TACACS, LDAP and web-based single sign-on.



RSA Identity Assurance Strategy & Roadmap

Findings Report identifying critical assets for risk mitigation with RSA two-factor and risk based authentication solutions

RSA ADVANCED CYBER DEFENSE PRACTICE

Readiness and resilience

Organizations need to know whether they are spending in the right areas and allocating scarce resources efficiently and effectively. RSA's battle-tested cybersecurity experts enable organizations to identify gaps, prioritize risks and design an operational program to systematically improve defenses, integrate solutions, provide deep visibility, detect advanced threats and reduce mitigation time. Services offered include:

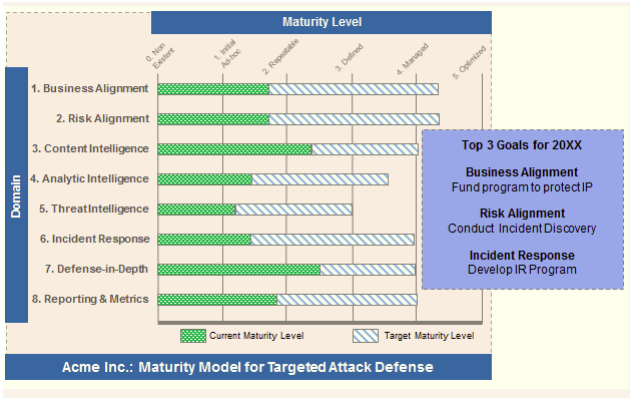
- *Strategy & Roadmap* - designed to identify gaps in current and target state maturity levels with comparison against peers for performance benchmarking.
- *SOC Design & Implementation* - development of technical and operational specifications and capabilities, including the use cases, staffing and resourcing models and run-books required to defend the organizational mission.

RSA INCIDENT RESPONSE PRACTICE

Early detection and rapid response

There's a narrow window of opportunity to prevent an adversary from carrying out his objectives after establishing a foothold in an organization. A well-designed Incident Response plan combined with RSA's IR Retainer services backed by on-demand cybersecurity experts can make all the difference to breach mitigation. Services leverage the RSA NetWitness Suite and include:

- *Incident Discovery* - designed to detect the types of vulnerability that enables threat actors to bypass traditional defense mechanisms.
- *IR Retainer* - a variety of service level options are available to provide customers with surge access to RSA IR expertise.
- *Incident Response* - the best technical expertise in the industry, designed to scope the nature and extent of an attack



RSA Strategy & Roadmap for Business Driven Security

Findings Report with benchmarking of current and target states for maturity across RSA's key domains for targeted attack defense

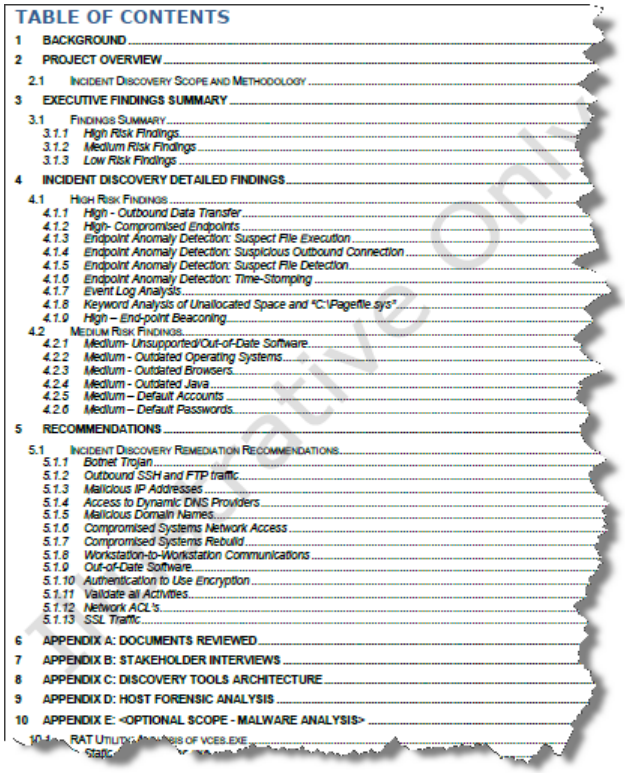


TABLE OF CONTENTS

1 BACKGROUND
2 PROJECT OVERVIEW
2.1 Incident Discovery Scope and Methodology
3 EXECUTIVE FINDINGS SUMMARY
3.1 Findings Summary
3.1.1 High Risk Findings
3.1.2 Medium Risk Findings
3.1.3 Low Risk Findings
4 INCIDENT DISCOVERY DETAILED FINDINGS
4.1 High Risk Findings
4.1.1 High - Outbound Data Transfer
4.1.2 High- Compromised Endpoints
4.1.3 Endpoint Anomaly Detection: Suspect File Execution
4.1.4 Endpoint Anomaly Detection: Suspicious Outbound Connection
4.1.5 Endpoint Anomaly Detection: Suspect File Detection
4.1.6 Endpoint Anomaly Detection: Time-Stomping
4.1.7 Event Log Analysis
4.1.8 Keyword Analysis of Unallocated Space and "C:\Pagefile.sys"
4.1.9 High – End-point Beaconing
4.2 Medium Risk Findings
4.2.1 Medium- Unsupported/Out-of-Date Software
4.2.2 Medium - Outdated Operating Systems
4.2.3 Medium - Outdated Browsers
4.2.4 Medium - Outdated Java
4.2.5 Medium – Default Accounts
4.2.6 Medium – Default Passwords
5 RECOMMENDATIONS
5.1 Incident Discovery Remediation Recommendations
5.1.1 Botnet Trojan
5.1.2 Outbound SSH and FTP traffic
5.1.3 Malicious IP Addresses
5.1.4 Access to Dynamic DNS Providers
5.1.5 Malicious Domain Names
5.1.6 Compromised Systems Network Access
5.1.7 Compromised Systems Rebuild
5.1.8 Workstation-to-Workstation Communications
5.1.9 Out-of-Date Software
5.1.10 Authentication to Use Encryption
5.1.11 Validate all Activities
5.1.12 Network ACL's
5.1.13 SSL Traffic
6 APPENDIX A: DOCUMENTS REVIEWED
7 APPENDIX B: STAKEHOLDER INTERVIEWS
8 APPENDIX C: DISCOVERY TOOLS ARCHITECTURE
9 APPENDIX D: HOST FORENSIC ANALYSIS
10 APPENDIX E: <OPTIONAL SCOPE - MALWARE ANALYSIS>

RSA Incident Discovery

Findings Report table of contents for an engagement where the RSA NetWitness Suite is used to identify anomalies which bypass traditional defenses

RSA PROFESSIONAL SERVICES

Product and technology deployment expertise

RSA Professional Services help organizations optimize their investments in RSA technologies, including:

- *RSA NetWitness Suite*
- *RSA Archer Platform*
- *RSA SecurID Suite*
- *RSA Identity Governance Suite*
- RSA Fraud & Risk Intelligence Suite

The portfolio includes services that accommodate differing requirements and maturity levels:

- *Design and Implementation services* - to get the solution up-and-running, achieve "early wins" and accelerate time-to-value.
- *Subscription services* - used annually to progress the maturity of the solution and work hand-in-hand with the customer to identify and implement use case requirements and enhance overall solution effectiveness.
- *Tuning & Optimization services* - recommended annually to maximize and tune solution performance, upgrade the environment to the latest release and implement additional features and functions.
- *Product integration services* - to accommodate the integration of RSA products with third party products and IT systems, such as IT ticketing.
- *Custom services* - tailored consulting for platform migrations, technology integration, high availability configurations, residencies and "expert-on-demand" staff augmentation.
- *Offshore services* - lower cost solution fulfillment by RSA's Virtual Services Delivery (VSD) team.

RSA UNIVERSITY

Cybersecurity Training Programs

RSA invests heavily in Research and Development, enabling our technologies to address the evolving threat environment and broader organizational security and risk management requirements. The continuing enhancement of security technology drives a need for specialized training and ongoing skills enhancement. RSA provides a combination of on-demand and instructor lead training to ensure that customers can enhance overall awareness, maximize the return on their product investments and optimize their cybersecurity capabilities.

PUTTING IT ALL TOGETHER

Enterprise-wide security program management

Protecting an organization's critical assets requires the right combination of technology and expertise. The RSA Risk and Cybersecurity Practice represents a team of battle tested security practitioners which are delivering solutions at scale on a global basis. When combined with RSA's industry leading technology portfolio organizations can avail of embrace the opportunities agility and efficiency presented by the latest development in IT while managing the risks to their business.

ABOUT RSA

RSA helps more than 30,000 customers around the world take command of their security posture by partnering to build and implement business-driven security strategies. With RSA's award-winning cybersecurity solutions, organizations can effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. For more information, go to https://www.rsa.com.

RSA