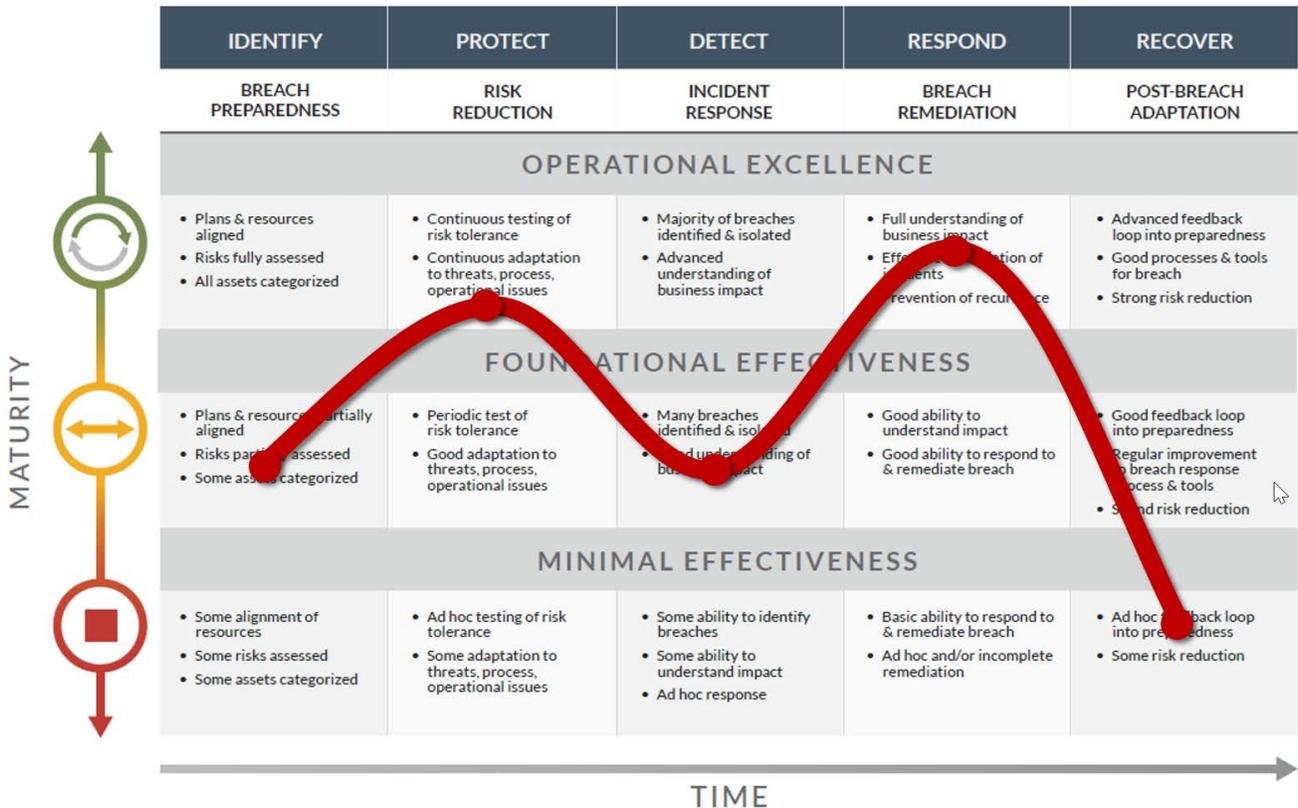


RSA® RISK FRAMEWORK FOR CYBER INCIDENT RISK

HELPS ORGANIZATIONS ASSUME CONTROL OF RISK FROM DIGITAL THREATS

Organizations are realizing that a new class of cyber and digital risks has emerged. These risks have their roots in traditional security, protection and risk challenges, but digital transformation has caused them to grow in scale, complexity and importance.

To help organizations improve their ability to manage these risks, RSA has developed RSA® Risk Frameworks. RSA Risk Frameworks are advanced assessment tools based on proven best practices for cybersecurity and risk management developed over thousands of previous engagements. They provide customers with a view of the current state of maturity and a roadmap for advancing maturity through consultative engagement. RSA Risk Frameworks are implemented by the RSA Risk & Cybersecurity Practice and provide customers with quantified risk scores that provide business-aligned solutions that target specific areas of risk maturity.





RSA CYBER INCIDENT RISK ASSESSMENT PROVIDES THE FOLLOWING:

- *Interviews and documentation with key business stakeholders to deeply understand the business's goals, objectives and existing risk posture*
- *Administration of the RSA proprietary Cyber Maturity Quantification tool to baseline current capacity*
- *Gap analysis of current state posture to desired levels of cyber maturity based on industry best practices*
- *Development of a roadmap that can be utilized to move to a desired level of cyber maturity*
- *Readout of results to stakeholders*

RSA Risk Framework for Cyber Incident Risk targets the difficult but critical task of protecting from digital threats that originate from both within and outside an organization. In an RSA-commissioned survey, 69% of IT security and business risk professionals indicated agreement or strong agreement that the relationship between business risk and IT security can be difficult to coordinate. Further, over 60% indicated agreement or strong agreement that their organizations have some weaknesses with regards to the IT and business risk management skills necessary for security breach detection and security breach response.¹

Consistent with industry-standard frameworks such as NIST Cybersecurity Framework (CSF) 1.1 and NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide (CSRC), RSA Risk Framework for Cyber Incident Risk helps organizations assess and improve their maturity across all of the core CSF processes: Identify, Protect, Detect, Respond and Recover. For each of these areas, RSA will apply its proprietary Cyber Maturity Quantification tool to develop a specific score relative to industry average. These distinct scores act as a tool to help organizations prioritize areas for improvement.

For more information or to schedule an assessment, contact your RSA sales executive or visit rsa.com/risk-frameworks.

ABOUT RSA GLOBAL SERVICES

The RSA Global Services team of 650 cybersecurity experts operates in more than 100 countries and earned a “Strong Performer” rating in the Forrester Wave™ for Digital Forensics and Incident Response Service Providers.² Over thousands of engagements, RSA Global Services has helped secure many types of organizations, often designing and implementing comprehensive risk and security management programs.

RSA Global Services combines deep security skills and broad risk management knowledge to help your organization assess and improve your cyber incident risk. Within the RSA Risk and Cybersecurity practice, two groups provide critical security capabilities:

- RSA Advanced Cyber Defense (ACD) delivers services to assess breach readiness, security operations center (SOC) or cyber incident response team (CIRT) assessment and design, incident response planning and testing, and “Expert on Demand” services.
- RSA Incident Response (IR) helps customers design, manage and perform incident response functions via both proactive and reactive services. Available on a retainer or ad hoc basis, RSA IR extends your organization’s security skills to deal with security incidents of all types and severities.

¹ ESG Custom Research, *Cybersecurity and Business Risk Survey*, June 2018

² Josh Zelonis, *The Forrester Wave™: Digital Forensics And Incident Response Service Providers*, Q3 2017, September 28, 2017² ESG Custom Research, *Cybersecurity and Business Risk Survey*, June 2018