TRAIL GUIDE TO NAVIGATING IDENTITY RISK

Access trails and environments are constantly changing. Perimeters are vanishing, user populations are mobile and outside the network walls, and IT can’t always confidently answer the question who has access to what and should they have that access?

Traditional IT and identity and access management (IAM) controls are no longer enough in today’s complex, dynamic IT environments.

Are you prepared to balance the demands of compliance and business agility? Read on for trail tips that can help you recognize—and reduce—critical identity risk factors.

WHAT’S AT RISK?

AUDIT PERFORMANCE SECURITY POSTURE USER PRODUCTIVITY

SPOTTING CRITICAL IDENTITY RISK FACTORS

First you need to identify and understand the hazards you’ll encounter on the path to addressing identity risk.

#1: Enable risk-aware and context-driven governance

Governance is key. Understand the business impact of application risk, privileged identities, and policy violations.

#2: Surface meaningful information for decisions

Prioritize actions based on risk and context so you can focus on the most critical actions first.

#3: Automate processes

Process orchestration for joiner-mover-leaver, rules, and birthright access all provide scale you need to manage risk, while ensuring appropriate response.

#4: Measure success

Track improvements to risk factors and deliver ROI on your identity governance investment.

SEE THE FOREST THROUGH THE TREES: AUTOMATING IAM WITH RISK CONTEXT

50% of companies’ are leveraging application risk data to automate IAM-related controls:

63% leverage approval workflows based on risk

58% execute and manage access certifications based on application risk categorization

42% perform step-up authentication based on an application’s risk rating

JOURNEY FURTHER: OPTIMIZING IDENTITY RISK MANAGEMENT WITH RSA

Optimizing your identity governance efforts helps you make better-informed, insight-driven security and compliance decisions, reducing enterprise risk and improving overall security.

• Expand visibility and control over multiple identities
• Increase efficiency with risk-prioritized actions
• Act with insight and context
• Save time and manual effort with automated processes
• Strengthen overall risk posture and reduce chances of audit failure or breach

With RSA® Identity Governance and Lifecycle, you know where your greatest risks lie and can mitigate them quickly. As you plan for growth, you can rest assured that user access is more secure and your business more compliant.

Learn more at RSA.com/igl

2016-17 EY Global Information Security Survey

1 2016-17 EY Global Information Security Survey