ARCHER

SOLUTION BRIEF

Archer® IT & Security Risk Management

As organizations increasingly rely on technology infrastructure to support digital initiatives, the complexity and scale of IT and security risk become more daunting. IT and security teams are already challenged with an increasing volume of security-related data created by layers of defense. Further complicated by the crushing mountain of business data they must protect, security and IT teams struggle to have a clear understanding of which data, systems and processes are most important to the business.

In addition, the adoption of cloud services, integration of external providers and expansion of business services create a significant challenge as organizations' perimeters have truly disappeared. Finally, the shadow of security threats has created an executive-level concern that reaches up to the board of directors level given the financial, reputational and regulatory exposure security breaches entail.

Bringing Insight to IT & Security

In order for IT risk and security functions to compile and render a complete picture of technology-related risk, multiple operational groups must collaborate and coordinate efforts. Security policies and compliance efforts must be aligned to regulatory and business requirements. Threat and vulnerability management processes must be agile to stay ahead of growing threats. Security operations must be active and diligent in order to swiftly identify active attacks against the organization and protect assets at risk. Today's security strategy must look beyond the immediate and tactical to bring innovative and cost-effective solutions to bear.

The Archer IT & Security Risk Management Advantage

With Archer® IT & Security Risk Management, your security function can benefit from enhanced visibility, analytics, action and metrics. You can determine which assets are critical to your business, establish and communicate security policies and standards, detect and respond to attacks, identify and remediate security deficiencies, and establish clear IT risk management best practices.

Connect cybersecurity risks in the context of integrated risk management

With interconnected business processes, organizations must be able to effectively address the complexity and cascading impact of rapidly changing cybersecurity risks. Archer IT & Security Risk Management can connect your security processes and data with risk and compliance functions across the enterprise. IT and security teams can then consider the relationship between business risk and IT risk in terms of business criticality to establish ownership and accountability, and connect IT and security risk to broader governance, risk and compliance programs.

Archer IT & Security Risk Management can connect your security processes and data with risk and compliance functions across the enterprise.

Address IT & Security Risk Management through multiple dimensions

To effectively manage IT and security risk, you must organize your security program in such a way that you can manage the full spectrum of technology-related risks—from policies, standards and compliance to threats, vulnerabilities and attacks. Archer IT & Security Risk Management enables IT and security teams to centrally manage processes, prioritize cyber threats and stay on top of the latest threats.

Bridge business context and process enablement

Managing IT and security risk today involves significantly more than just deploying defensive technologies. IT risk must be understood in business terms since technology issues could put the entire organization at serious risk. Archer IT & Security Risk Management bridges the gap between people and technology by establishing processes to identify and escalate risks effectively and efficiently. By ensuring alignment between the business and IT, your IT and security risk management program can facilitate what needs to be addressed to keep the business secure.

Archer IT & Security Risk Management

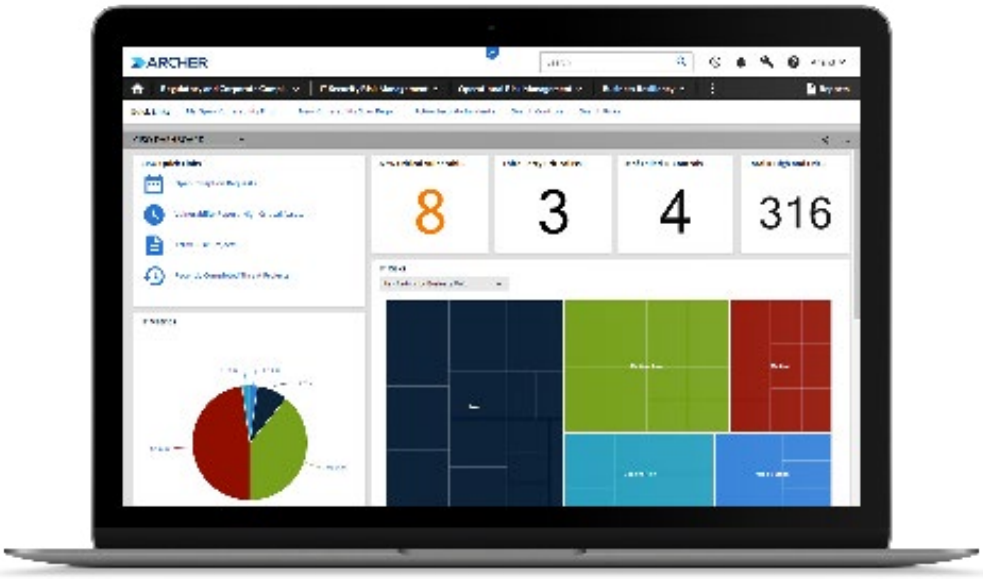
Archer IT & Security Risk Management enables you to evaluate which assets are critical to your business, establish and communicate security policies and standards, detect and respond to attacks, identify and remediate security deficiencies, and establish clear IT risk management best practices. It includes a number of use cases to meet your specific needs:

- **Archer Issues Management** allows you to capture and consolidate issues that arise, including security incidents,failed or deficient internal controls and exceptions that require attention or escalation. Robust reporting makes it easy for the board and all levels of management to understand the full scope of outstanding issues, priorities and remediation timelines.
- **Archer IT & Security Policy Program Management** allows you to effectively manage the entire policy development lifecycle process and provides the framework for establishing a scalable and flexible environment to manage corporate and regulatory policies and ensure alignment with compliance obligations. Out-of-the-box content includes the most current security frameworks and control catalogs.

- **Archer IT Controls Assurance** enables you to assess and report on the performance of controls across all IT assets and automate control assessment and monitoring. You can implement a centralized system to catalog IT assets for compliance reporting and establish a system of record for documenting IT controls.
- **Archer Cyber Risk Quantification** allows you to quantify the financial risk exposure to cybersecurity events. Armed with this financial data, your organization can make more informed decisions regarding risk and security investments.
- **Archer Cyber Incident & Breach Response** enables you to centrally catalog organizational and IT assets, establishing business context to drive incident prioritization and implement processes designed to escalate, investigate and resolve declared incidents effectively. It is designed to help bridge the gap between your security operations teams and IT and the business and allow security managers to stay on top of the most pressing issues.
- **Archer IT Security Vulnerabilities Program** takes a big data approach to helping security teams identify and prioritize high-risk threats. You can proactively manage IT security risks by combining asset business context, actionable threat intelligence, vulnerability assessment results and comprehensive workflows.
- **Archer IT Risk Management** allows you to catalog organizational elements and IT assets for IT risk management purposes. It includes a risk register to catalog IT risks, prebuilt risk assessments for IT, a prebuilt threat assessment methodology and a catalog to document IT controls.
- **Archer PCI Management** allows you to streamline the Payment Card Industry (PCI) compliance process, automate assessments and reduce the effort required to comply. You can jump start your PCI compliance program with an organized project management approach, efficiently conduct continuous assessments, and gain the visibility needed to manage and mitigate risk.
- **Archer IT Regulatory Management** provides the necessary tools and capabilities to document external regulatory obligations that impact your IT and sensitive data environments, allowing your organization to keep pace with changing business and IT compliance risk.
- **Archer CMMC Management** enables organizations to identify, document, and manage the appropriate CMMC practicesand processes required for improved cybersecurity hygiene for storage and management of CUI (controlled unclassified information) data, to help meet the challenges of CMMC certification.
- **Archer Information Security Management System (ISMS)** enables you to quickly scope your information security management system and document your Statement of Applicability for reporting and certification purposes. Any issues identified during assessments can be centrally tracked to ensure remediation efforts for gaps are consistently documented, monitored and effectively addressed.

Archer IT & Security Risk Management bridges the gap between people and technology by establishing processes to identify and escalate risks effectively and efficiently.

Archer IT & Security Risk Management provides a business risk-based approach to security to help reduce the risk of today's security threats, misaligned security practices and operational security compliance failures. You can establish business context for security, document and manage security policies and standards, detect and respond to attacks, and identify and remediate security vulnerabilities.



Discover More

Archer is a leading provider of integrated risk management (IRM) solutions that enable customers to improve strategic decision-making and operational resilience with a modern technology platform that supports qualitative and quantitative analysis driven by both business and IT impacts. As true pioneers in GRC software, Archer remains solely dedicated to helping customers manage risk and compliance domains, from traditional operational risk to emerging issues such as ESG. With over 20 years in the risk management industry, the Archer customer base represents one of the largest pure risk management communities globally, with more than 1,200 customers including more than 50% of the Fortune 500.

Visit www.ArcherIRM.com.

@ArcherIRM Archer Integrated Risk Management

ARCHER