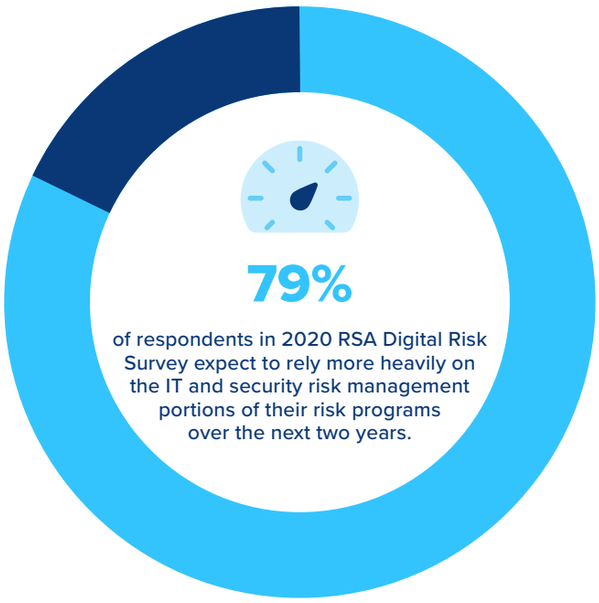
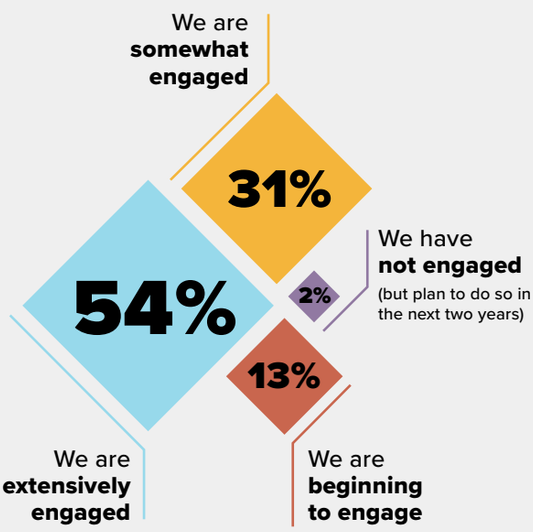
Achieving Operational Resilience:
Don't stop at IT and Security Risk Management

The rapid expansion and adoption of technology creates a massive and dynamic risk landscape and organizations need integrated risk management to protect their business.



TO WHAT EXTENT HAS YOUR ORGANIZATION ENGAGED IN DIGITAL TRANSFORMATION INITIATIVES OVER THE PAST TWO YEARS?



THE IMPORTANCE OF IT RISK MANAGEMENT IN AN INTEGRATED RISK MANAGEMENT STRATEGY

Of the 1100+ Archer deployments for IT and security risk management, over 80% of those customers also utilize compliance processes on the Archer platform.

Over 70% of our early stage deployments target IT and security risk use cases highlighting the foundational role that IT risk management can play in an IRM strategy.

We recommend organizations prepare for and orchestrate coordinated security, IT and business response to the attack to stop the threat and minimize business impact.

We recommend organizations compile a complete picture of technology and security-related risks and understand their financial impacts.

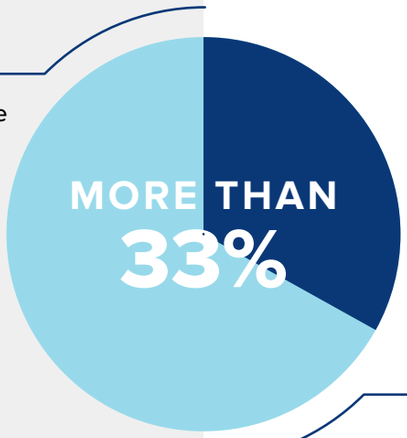
While many faced a moment of reckoning around risk during the pandemic, a lucky few were able to quickly adapt and thrive. Get the lessons learned from Archer's customers to discover why an integrated risk management approach focused on operational resilience can help companies like you get better prepared for disruptions and risk.

GET REPORT

Achieving Operational Resilience:
Businesses must go beyond compliance.

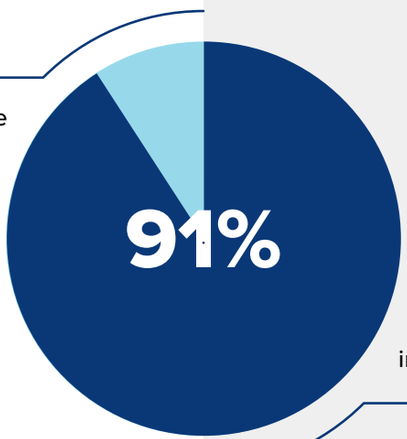
An integrated risk approach that weaves together risk functions not only ensures compliance but also helps to achieve strategic business goals.

More than 33% of respondents in the 2020 RSA Digital Risk Survey stated integrated third-party risk and enterprise risk management approaches is their number 1 priority regarding vendor and supply chain risk.



More than 33% of respondents in the 2020 RSA Digital Risk Survey stated a risk-based compliance methodology is a priority for them in the next two years.

91% of Archer customers that license enterprise and operational risk management (EORM) use cases also license compliance use cases. In addition, customers who license EORM use cases are five times more likely to also own audit use cases.



The usage of EORM, Compliance and Audit use cases substantiates the close connection between these fundamental processes and the importance of an integrated approach.

We recommend bringing together disparate components of a compliance program into a cohesive unit gives your company a clear line of sight into the laws & regulations you need to be concerned with.

We recommend organizations establish tools and techniques to ensure all three lines of defense (front-line managers, risk and compliance teams, and independent audit) have clear roles and responsibilities.

Download our whitepaper "The State of Risk Management" to discover the four themes to achieving operational resilience now and in the future in order to not only survive, but thrive in times of upheaval.

GET REPORT

ARCHER

State of Integrated Risk Management Report

Achieving Operational Resilience:
Measure with Quantification, Mature with Focus

Integrated risk management is a journey - not a destination. Through quantification and disciplined evolution - you can make sure your business resiliency and program are maintaining the right momentum.

QUANTIFICATION IS THE BEST WAY TO CALCULATE RISK

Qualitative measures usually consider risks one by one (instead of in aggregate) and miss the bigger picture.

Quantification provides a more flexible, mathematical language that allows risk managers to calculate, correlate, and communicate their cyber risk in the standard business language of money.

With the right technology, risk quantification becomes accessible, understandable, and actionable and is possible regardless of risk management maturity or the amount of data in place.

KEEP MOVING FORWARD

Organizations just starting on their IRM journey should first look to streamline compliance or focus on one type of risk (IT, vendor, BC/DR, etc.) to build momentum.

Organizations that have established programs in individual domains should be working to expand their risk focus and improve visibility, analysis, and metrics.

Organizations with well-structured programs continue to need to connect risk to the business with cross-functional processes.

Download "The State of Risk Management" to discover why organizations of all sizes must embrace an integrated risk management approach focused on operational resiliency to survive the evolving risk landscape.

GET REPORT