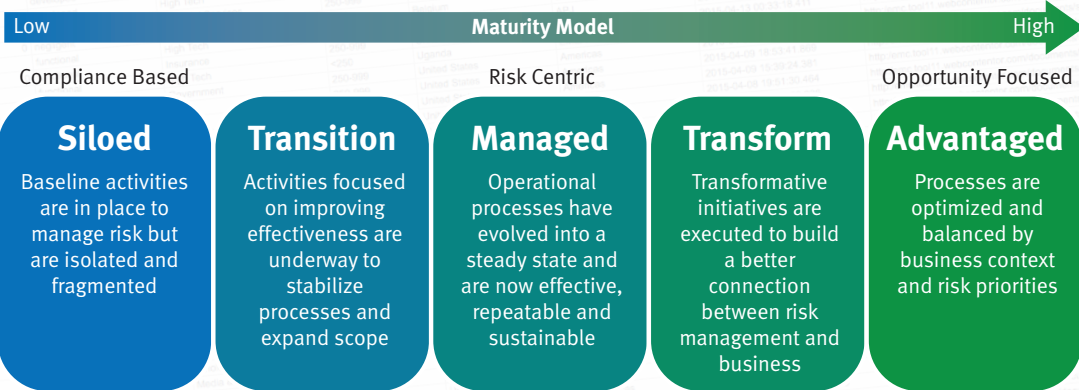# RSA® Archer™
Risk Intelligence Index

RSA®

OVERVIEW

In October 2015, RSA completed a global survey of almost 400 organizations to gather insight into current trends and perceptions regarding Risk Management. The survey utilized RSA's proprietary Risk Intelligence Index to ask questions around key areas of risk and how organizations are addressing the changing risk landscape. The Risk Intelligence Index is based on the RSA Archer Maturity Model that measures organizations' GRC program components across five stages of maturity.
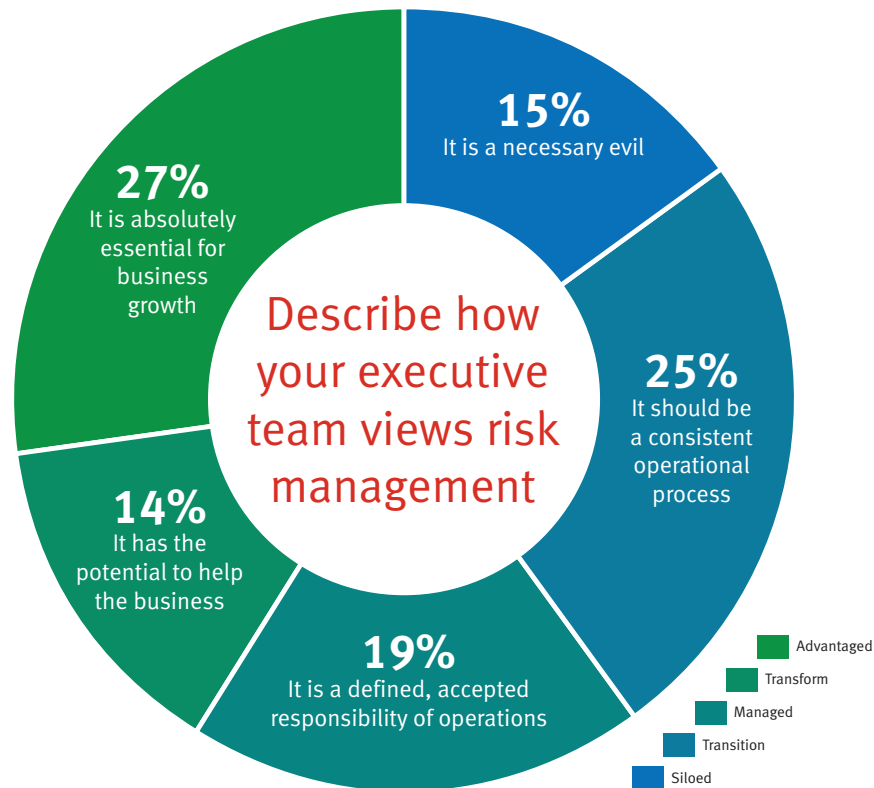
Low	Maturity Model	High

Compliance Based | Risk Centric | Opportunity Focused

Siloed	**Transition**	**Managed**	**Transform**	**Advantaged**
Baseline activities are in place to manage risk but are isolated and fragmented	Activities focused on improving effectiveness are underway to stabilize processes and expand scope	Operational processes have evolved into a steady state and are now effective, repeatable and sustainable	Transformative initiatives are executed to build a better connection between risk management and business	Processes are optimized and balanced by business context and risk priorities

OVERALL ORGANIZATIONAL ATTITUDE TOWARDS RISK

Key Finding

Approximately **40%** of the respondents' executives view risk management as an ingredient to business success. **60%** still see risk management as an operational problem.
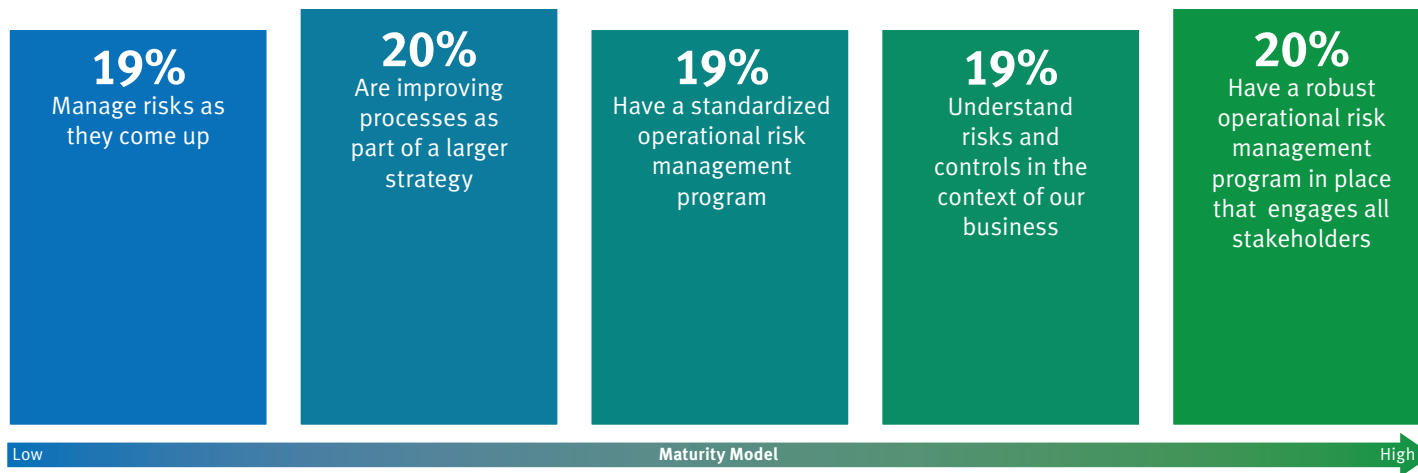
Key Recommendation

Risk Management functions need to connect every effort to the business strategy to raise awareness and educate executives on how risk management can accelerate business growth.

Describe how your executive team views risk management

15%
It is a necessary evil

25%
It should be a consistent operational process

19%
It is a defined, accepted responsibility of operations

14%
It has the potential to help the business

27%
It is absolutely essential for business growth

- Advantaged
- Transform
- Managed
- Transition
- Siloed

OPERATIONAL RISK MANAGEMENT

When it comes to managing risks within business operations, we

19% Manage risks as they come up	**20%** Are improving processes as part of a larger strategy	**19%** Have a standardized operational risk management program	**19%** Understand risks and controls in the context of our business	**20%** Have a robust operational risk management program in place that engages all stakeholders

Low   **Maturity Model**   High

Key Finding
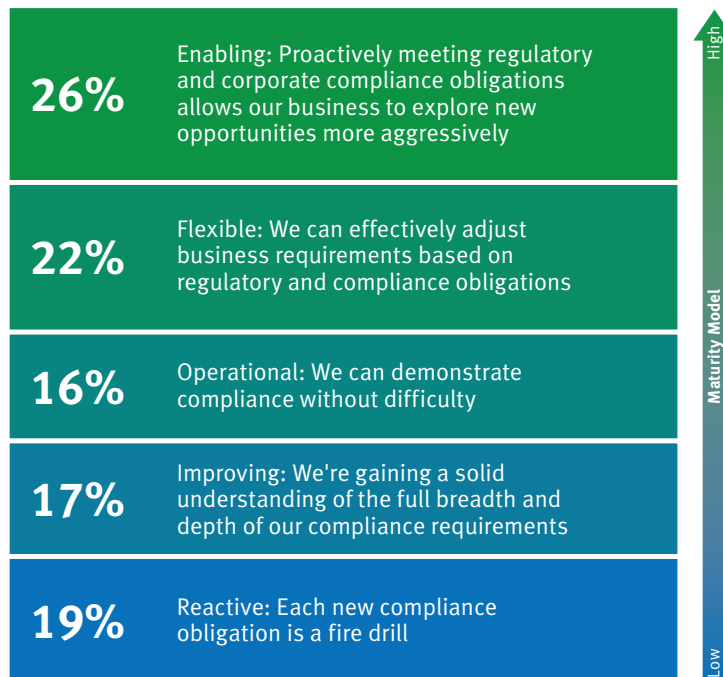
Although **4/5** of respondents have ORM in place, the survey results indicate an equal distribution of operational risk management maturities.

Key Recommendation

Organizations should strive to understand the full business context of their risks and controls to get the most out of the risk management program.

REGULATORY & CORPORATE COMPLIANCE

Our regulatory and corporate compliance efforts are:

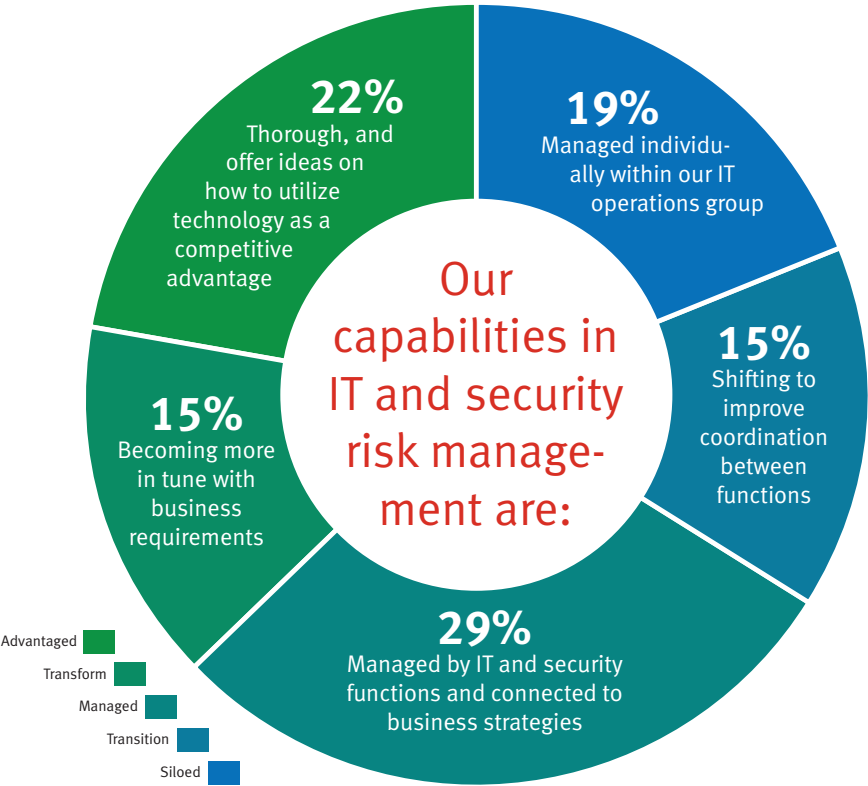|	
26%	Enabling: Proactively meeting regulatory and corporate compliance obligations allows our business to explore new opportunities more aggressively
22%	Flexible: We can effectively adjust business requirements based on regulatory and compliance obligations
16%	Operational: We can demonstrate compliance without difficulty
17%	Improving: We're gaining a solid understanding of the full breadth and depth of our compliance requirements
19%	Reactive: Each new compliance obligation is a fire drill

High

Maturity Model

Low

Key Finding

Respondents reported an almost equal split between respondents that are anticipating regulatory changes as those that continue to react as a compliance exercise.

Key Recommendation

Organizations should implement continuous controls monitoring in conjunction with risk-based compliance to gain program efficiencies.

IT AND SECURITY RISK MANAGEMENT

22%
Thorough, and offer ideas on how to utilize technology as a competitive advantage

19%
Managed individually within our IT operations group

Our capabilities in IT and security risk management are:

15%
Shifting to improve coordination between functions

15%
Becoming more in tune with business requirements

29%
Managed by IT and security functions and connected to business strategies

- Advantaged
- Transform
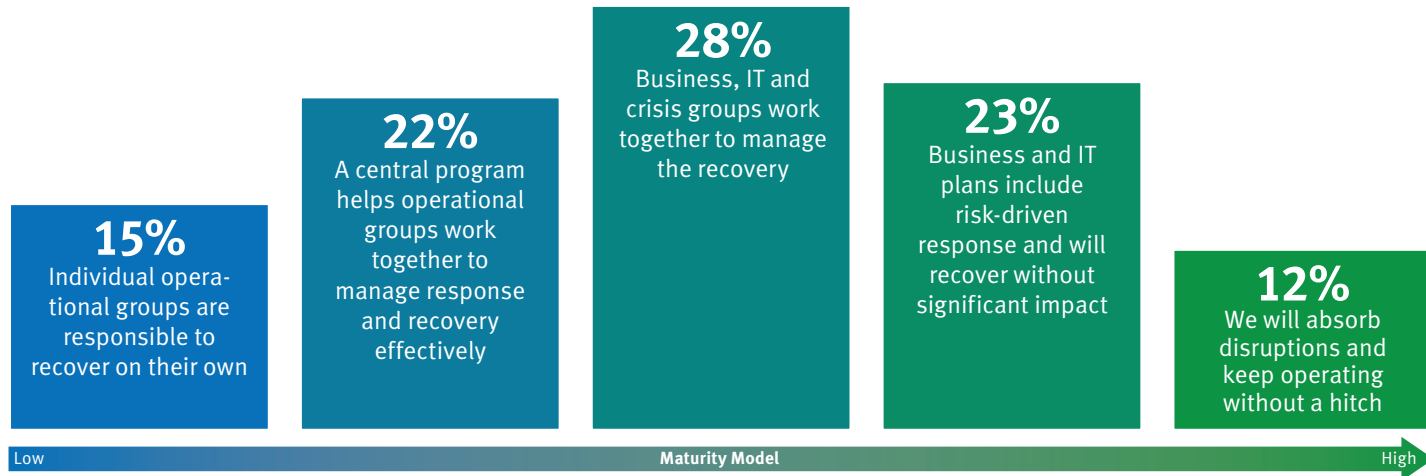- Managed
- Transition
- Siloed

Key Finding

Only **22%** of the respondents indicated that they are able to use IT and Security Risk Management as a competitive advantage.

Key Recommendation

IT and Security functions should build business context around security issues and ensure IT and security risks are connected to overall operational and enterprise risk strategies.

BUSINESS RESILIENCY

If there is a disruption within business operations:

15%
Individual operational groups are responsible to recover on their own

22%
A central program helps operational groups work together to manage response and recovery effectively

28%
Business, IT and crisis groups work together to manage the recovery

23%
Business and IT plans include risk-driven response and will recover without significant impact

12%
We will absorb disruptions and keep operating without a hitch

Low   Maturity Model   High
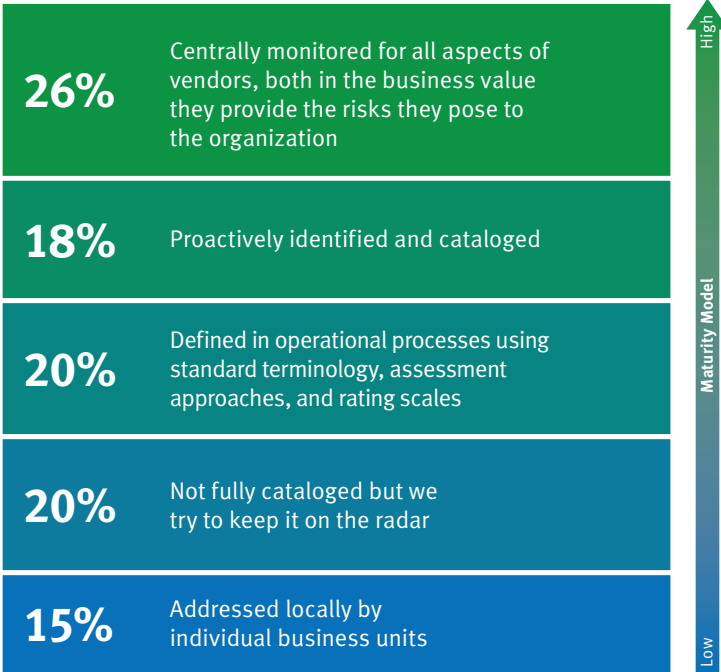
Key Finding

85% of the respondents have a central or coordinated program for recovery, but only **1/3** indicate true confidence in managing their business resiliency risk.

Key Recommendation

To drive confidence in resiliency, organizations need to have a central program, collaboration among recovery functions, and take risk-based approaches.

THIRD PARTY GOVERNANCE

Third-party risk is:

26%	Centrally monitored for all aspects of vendors, both in the business value they provide the risks they pose to the organization
18%	Proactively identified and cataloged
20%	Defined in operational processes using standard terminology, assessment approaches, and rating scales
20%	Not fully cataloged but we try to keep it on the radar
15%	Addressed locally by individual business units

High

Maturity Model

Low

Key Finding

Third party risk is one of the fastest rising issues and **1/3** of the respondents indicate low maturity in addressing third party risk.

Key Recommendation

Organizations with low maturity should establish a maturity roadmap and engage stakeholders across the organization in the third-party governance program.

AUDIT MANAGEMENT

Key Finding

77% of respondents reported that their audit activities were risk-based to adjust based on business changes.
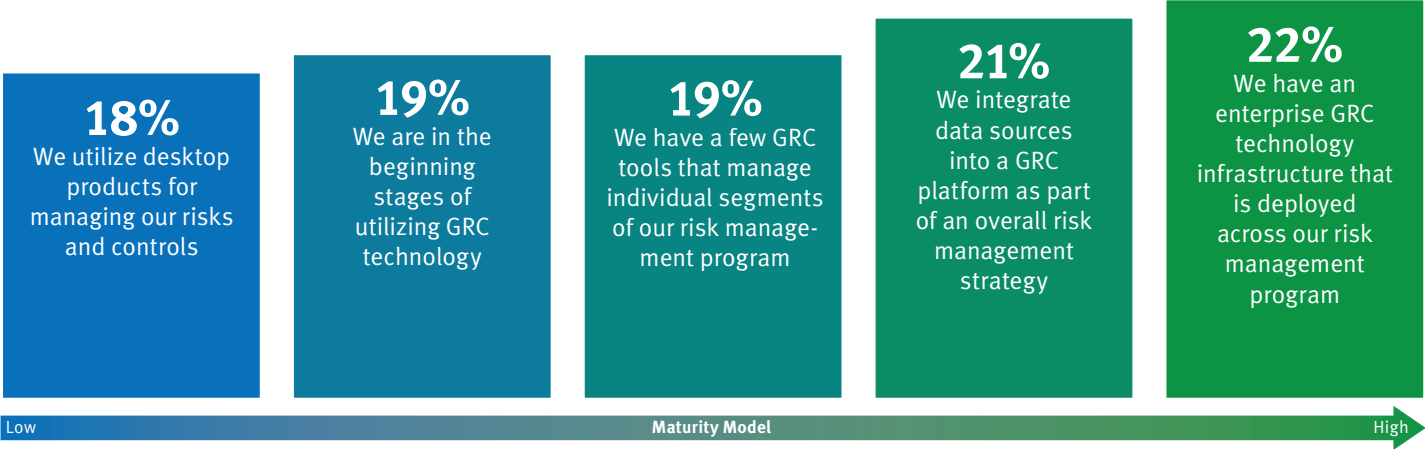
Key Recommendation

Internal Audit (IA) should leverage insight from Enterprise and Operational Risk Management to dynamically adjust audit plans and engagements in response to changing business conditions.

We ensure our controls are working effectively by:

28%
Dynamically assessing risks and monitoring key controls continuously

23%
Performing basic compliance audits on an ad-hoc basis

16%
Using static analysis of risk and criticality to plan and execute audits

12%
Leveraging flexible audit processes that can adjust to shifting risks

21%
Using an established audit function to conduct risk-driven reviews

Advantaged
Transform
Managed
Transition
Siloed

GRC TECHNOLOGY USAGE

Describe how technology supports your GRC program:

18%
We utilize desktop products for managing our risks and controls

19%
We are in the beginning stages of utilizing GRC technology

19%
We have a few GRC tools that manage individual segments of our risk management program

21%
We integrate data sources into a GRC platform as part of an overall risk management strategy

22%
We have an enterprise GRC technology infrastructure that is deployed across our risk management program

Low   **Maturity Model**   High

Key Finding

Respondents indicate there is still a wide variety of maturities in utilizing technology to support the GRC program.

Key Recommendation

Organizations must look for an integrated technology strategy to create a cohesive picture of risk.

OVERALL RISK INTELLIGENCE MATURITY

Due to pressures from boards and executives, organizations are actively looking to drive more mature Risk Management programs but **less than 10%** of respondents reached the most mature state in RSA's Risk Maturity Index. All respondents noted at least one dimension of risk management that needed improvement.

Facing a more volatile risk environment, organizations must continue to improve GRC initiatives to transform compliance, focus more on risk, and ultimately help the business drive growth.

2% Siloed

9% Advantaged

15% Transition

Aggregated score across all 5 stages

38% Transform

36% Managed

EMC²

RSA