RSA® ARCHER® MATURITY MODEL: RISK INTELLIGENCE INDEX

OVERVIEW

Today’s business environment is fraught with risk. Economic, technology and market conditions affect organizations on a daily basis. The constantly “changing risk landscape” is a discussion point in headlines, industry forums, media outlets and board rooms. The RSA® Archer® Risk Intelligence Index is a simple measurement of the six major dimensions of risk management that organizations must address in order to turn risk into a competitive advantage to fuel the enterprise.

CONTENTS

Why Risk Intelligence? 2
Risk Challenges....................3
Risk Practices....................4
The RSA Archer Risk Intelligence Index....................5
Conclusion....................10
About RSA Archer Maturity Models 10

RSA Whitepaper

WHY RISK INTELLIGENCE?

Today's business environment is fraught with risk. Economic, technology and market conditions affect organizations on a daily basis. The constantly "changing risk landscape" is a discussion point in headlines, industry forums, media outlets and board rooms. We are moving to a world where risk management will become the primary source of competitive advantage. Rather than avoiding risk, organizations need the ability to embrace risk with confidence.

Risk management will become the core capability which separates winners from losers. Organizations that understand and manage risk effectively will prosper, while those that can't will fail. Success starts with the ability to manage operational risk in a manner that frees up resources to focus on the company's long term, strategic objectives. Risk Intelligence gives companies the confidence to harness risk to explore new opportunities.

Executives need relevant, up-to-date information to make the right decisions and pursue the right opportunities. RSA Archer's Risk Intelligence approach represents a balanced approach to manage the major risks facing organizations today and provide the insight to make the right business decisions, address risk and explore new opportunities with predictability. RSA Archer can be the backbone of your operational risk and compliance management program. By sharing data, leveraging processes and breaking down organizational barriers, RSA Archer builds efficiencies across the organization to effectively transform compliance, manage risk and exploit opportunity.

RSA Archer GRC Maturity Models focus on key capabilities enabled by the RSA Archer solution. As a technology enabler, RSA Archer provides the critical infrastructure to leverage processes, share data and establish common taxonomies and methodologies.

Whether they like it or not, all Risk and Compliance functions are expected to add value to the organization. These days, you can't invest in anything that doesn't bring value to the company. Risk and Compliance functions are no different. The Risk Intelligence Index uses two simple measurements to articulate the value of the GRC program to the organization. The first is Results; GRC programs are expected to drive a constant increase of effectiveness in managing risk and compliance. There also has to be a continued expansion of Reach. As the risk and compliance function matures, ideally it protects more and more of the organization. These two factors, as they increase, are key measurements of the risk and compliance function and how it brings Value to the organization.

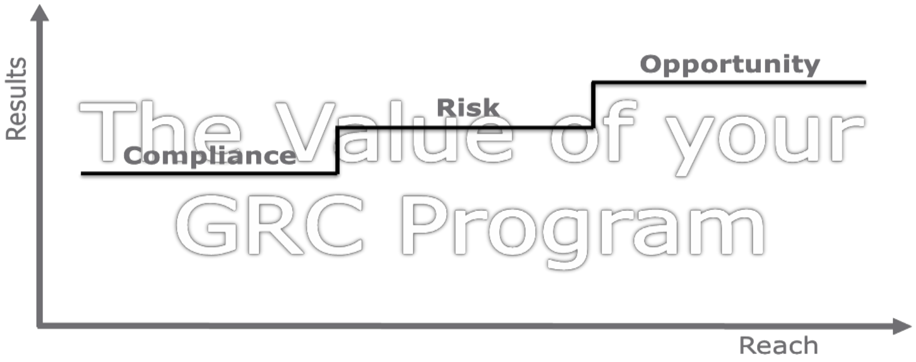


Figure 1. GRC Program Value

Organizations are looking to improve their results and expand their reach to increase value. They do it by moving up the "stairs." The first step is meeting the company's Compliance obligations. Most organizations have achieved a certain level of results and are expanding their compliance reach. The second step in moving up the stairs is managing Risk. Ultimately, the goal is to reach the point where the organization can use Compliance and Risk as a competitive advantage – truly bringing value to the organization by helping to drive Opportunity

RISK CHALLENGES

Factors such as compliance velocity and complexity, organizational size, structure and geographic footprint, business models and technology usage and strategy play large roles in the risk profile of an organization. When an organization looks at its broad strategy around risk management, these elements will drive the level of maturity necessary for effective reduction of risk.

Compliance Environment
Depending on the industry, geographic location or business products and services, companies face a wide variety of compliance obligations. The complexity of the compliance environment is not necessarily associated with just the size of the organization. A small company, in a highly regulated industry such as financial services, can face a significantly complex regulatory environment. Alternatively, a large company may deal with a smaller regulatory and compliance environment. Factors to consider include:

- Complexity and velocity of regulatory and/or industry obligations
- Number and nature of regulators
- Frequency of audits
- Rate of regulatory change

Geographic Distribution
The geographic locations included in a company's footprint will play a role in the risk challenge. Large distributed companies face challenges such as language, logistics, culture and communication barriers that smaller, regional companies will not necessarily face. The location of third party suppliers, distributors and other partners must be included when assessing the overall geographic distribution of the company.

Complexity of Business
The business model and strategy will play a significant role in determining the level of maturity necessary for a company to manage risk appropriately. Companies with highly complex business models with numerous products, services, external relationships and customer profiles must address a wider range of operational risks.

Size of Organization
The overall size of the organization, both in terms of employees and revenue will factor into the risk challenge.

Significant Events
Companies with a history of significant risk events (compliance failures, fines, disruptions, losses or near misses) face a higher risk profile. In addition, those companies whose peers or competitors that have had significant events indicate a higher risk within the overall industry.

Technology Profile
A complex Information Technology infrastructure faces a higher rate of possible risks. Factors such as outsourcing, usage of third parties, cloud service providers and the extended enterprise will contribute to significant technology oriented risks.

Organizational Dynamics

Companies with a high rate of change in organizational structure or turnover, e.g. seasonal employees, face complexities in education, culture, awareness and retention of institutional knowledge.

Technology Usage

Companies that are the cutting edge of technology - adopting or innovating new uses of any technology - will face a higher set of possible risks. This should not just include Information Technology but other technology categories based on the nature of the business, e.g. new manufacturing technologies or innovative products.

These dynamics are addressed within the Risk Intelligence Index by identifying an overall level of Risk Challenge. The Risk Challenge level indicates whether the organization faces Minimal, Moderate, Significant or Serious obstacles or barriers in implementing an enterprise class risk management program.

RISK PRACTICES

The Risk Intelligence Index is based on two sets of measurements – Foundations and the Six Dimensions of Risk Intelligence.

Foundations

Foundations are critical elements necessary for the overall success of the Maturity Journey. Without these foundations in place, the organization will face difficulties throughout the journey either through the lack of focus, commitment, resources or strategy.

The Foundations include:

- Level of performance and risk acceptable by management
- Expectations and success criteria for risk management
- Importance on the maturity of risk processes
- Budget and resources
- Culture/Formalization of accountability

Six Dimensions of Risk Intelligence

The RSA Archer Risk Intelligence Index focuses on the six major risk areas that organizations must address when building Risk Intelligence:

- Operational Risk
- Regulatory and Corporate Compliance
- IT Security Risk
- Third Party Governance
- Business Resiliency
- Audit Management

Each dimension is measured based on two factors of the existing processes and capabilities within the organization. Risk practices are measured for Effectiveness and Organizational Reach using the following scales:

Effectiveness
Not Implemented — The activity is not currently executed.

Isolated — The activity is executed but is done so inconsistently. Limited to no technology utilized.

Consistent — The activity is executed in a repeated manner. Technology used but in a disconnected/decentralized manner.

Defined — The activity is consistently executed and documented. Technology used for centralization and coordination.

Measurable — The activity is defined and monitored for performance. Technology centralizes data and manages processes for analysis and metrics.

Optimized — The activity is consistently measured and continuously improved. Technology used to identify and track performance indicators.

Organizational Reach
Non-existent — The activity is not currently executed.

Local — The activity is executed but is performed differently across organizational elements and locations. Technology is implemented and utilized only at the local level.

Fragmented — The activity is executed in similar manners but is not defined and is erratic across organizational elements and locations. Some common tools/technologies are utilized.

Persistent — The activity is generally consistent across organizational elements and locations. Technology plays a role in establishing taxonomies and processes.

Pervasive — The activity is consistent across the entire organization. Centralized or enterprise technology platforms enable common processes and data stores.

A key part of the measurement of these Effectiveness and Organizational Reach levels is the use of technology as an enabler. Processes supported by common technology tools that establish common data stores, enforce taxonomies and drive consistencies will generally be more effective and allow the processes to affect a larger part of the organization.

THE RSA ARCHER RISK INTELLIGENCE INDEX

Risk Challenge Level
Based on the level of Risk Challenges, the organization is rated on a four level scale indicating the overall nature of the barriers facing the risk and compliance strategy. The four levels are:

Minimal – Companies with "Minimal" risk challenges have limited obstacles in managing risk due to a smaller size, scope and complexity. These types of companies should focus on practices that are cost effective and understanding of the limited resources while maintaining a proactive risk management program.

Moderate – Companies with "Moderate" risk challenges face some obstacles in managing risk. These companies should focus on effective practices that reduce risk while balancing effort with return on investment.

.

Significant -- Companies with "Significant" risk challenges face obstacles in managing risk due to complexities of the business. These companies should focus efforts on broad program elements that are effective and efficient maintaining a solid level of flexibility to adjust controls based on changing risks.

Serious – Companies with "Serious" risk challenges face the most obstacles in managing risk due to the size, scope and complexity of the organization. Companies with these challenges must look to build extensible risk management programs that take into account the complicated and volatile risk landscape.

Overall Risk Intelligence Index

The Risk Intelligence Index is a measurement of the current risk management practices. The Index is segmented into four quadrants based on Results and Reach.

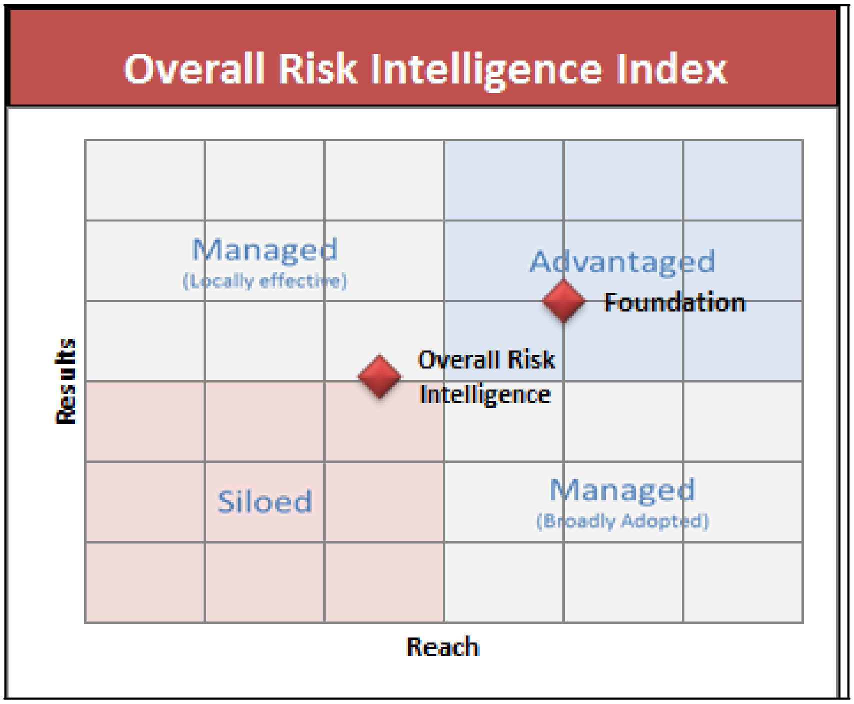


Figure 2. Overall Risk Intelligence Index

The Results axis is based on the Effectiveness of current processes. Organizations with practices that are Defined, Measurable or Optimized will score higher on the Results axis. These values of process effectiveness indicate a higher level of maturity - processes are documented, consistent and repeatable.

The Reach axis is based on the Organizational Reach of existing processes. Organizations with processes that are Persistent or Pervasive will score higher on the Reach axis. This indicates that processes have been implemented across organizational boundaries. While processes may not be identical within operating units, risk management is collectively more mature when adoption rates are higher.

The Quadrants

Siloed -- This quadrant indicates the organization is the initial stage of managing risk. Practices are not yet effective and not adopted across organizational boundaries. Companies in the Siloed stage should look to improve the effectiveness of processes through documentation and automation. As processes become more effective locally, the practices can be extended to more parts of the organization reducing overall risk.

Managed (Locally Effective) – This quadrant indicates processes have achieved a strong level of effectiveness but are not adopted across the organization. Companies in this quadrant should look to promote these effective processes and foster a culture of adoption to reduce risks across operational boundaries.

Managed (Locally Effective) – This quadrant indicates processes have achieved a strong level of effectiveness but are not adopted across the organization. Companies in this quadrant should look to promote these effective processes and foster a culture of adoption to reduce risks across operational boundaries.

Managed (Broadly Adopted) – This quadrant indicates processes have crossed operational boundaries but are not yet as effective as necessary to reduce risk. Companies in this quadrant should look at ways of improving the execution of risk management processes through automation or stronger governance.

Advantaged – This quadrant indicates the highest level of maturity. Processes are effective and adopted across the organization. Companies in this quadrant should look to sustain their practices and look for efficiencies to lower costs while maintaining a strong risk management posture.

The Overall Risk Intelligence Index is plotted based on the Effectiveness and Organizational Reach of the current practices. The Overall Risk Intelligence Index is a quick, easy method to measure an organization's overall maturity level. Individual scores for the Six Dimensions highlight gaps in current aspects of the risk management practices. Dimensions low on the Results and Reach (in the Siloed quadrant) indicate opportunities to raise the overall risk intelligence through targeted improvements.

Dimensions in the "Managed (Broadly Adopted)" quadrant can improved by RSA Archer through more effective processes and better execution. Dimensions in the "Managed (Locally Effective)" quadrant can be driven across the organization by RSA Archer enforcing common taxonomies and processes and sharing data.

The Foundation score is plotted based on the rating of the Foundation questions. The Foundations score is also an indicator to the level of success and sustainability of the overall program. If the Foundation score is higher on the scale than the Overall RII (or individual Dimensions), it indicates an openness and interest in raising the overall Risk Intelligence of the organization. Efforts will see better commitment from Management in improving risk practices. If the Foundation score is lower on the scale than the Overall RII, the organization will face barriers in sustaining the current program.

Domain Risk Intelligence Indices

The Domain Risk Intelligence Indices (Figure 3) plots the individual dimensions of Risk Intelligence in the same quadrant system. The quadrant system makes it easy to identify dimensions of risk management that are lagging or reducing the overall capabilities of the organization to manage risk.

This graph can be used to identify several areas of discussion:

- Highlight areas of risk management that are lagging. Dimensions low on the Results and Reach (in the Siloed quadrant) indicate opportunities to raise the overall risk intelligence through targeted improvements. The implementation of RSA Archer will improve both Results and Reach by establishing a common platform for risk management.

- Highlight areas where Effectiveness must be improved. Dimensions in the “Managed (Broadly Adopted)” quadrant can be improved by RSA Archer through more effective processes and better execution. RSA Archer can automate processes, eliminate manual, duplicative and error prone processes and enable broadly adopted practices to become more operational.
- Highlight areas of where Reach must be expanded. Dimensions in the “Managed (Locally Effective)” quadrant can be expanded across the organization with RSA Archer enforcing common taxonomies and processes and sharing data. With a common platform in place to leverage processes and data, adoption of effective practices is more easily driven across the organization.

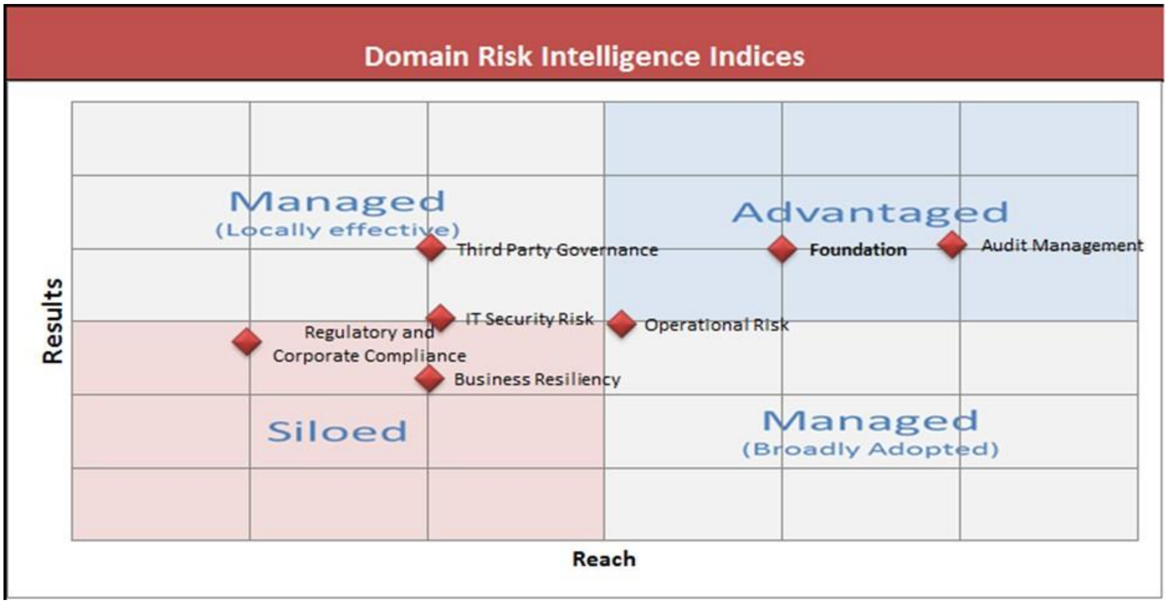


Figure 3. Domain Risk Intelligence Indices

Domain Coverage

The Domain Coverage graphs show the individual dimensions of Risk Intelligence broken out by Results and Reach. This is a further breakdown showing the gaps in the optimal state for each Dimension.

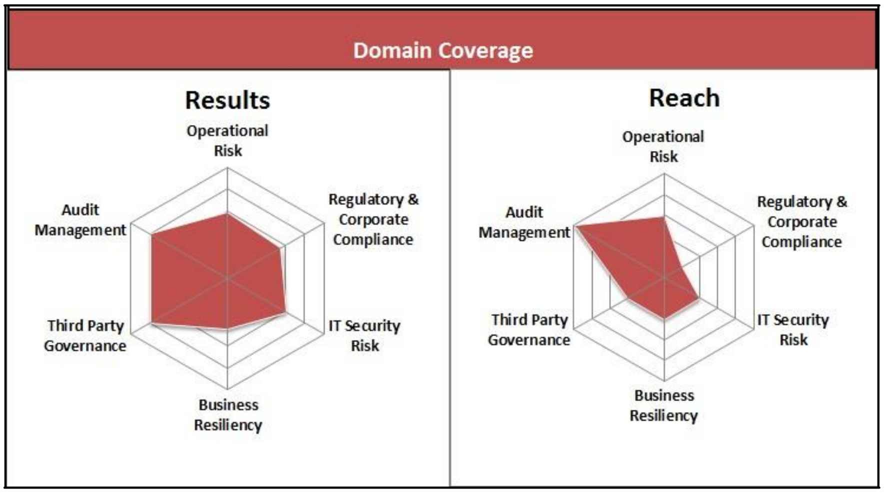
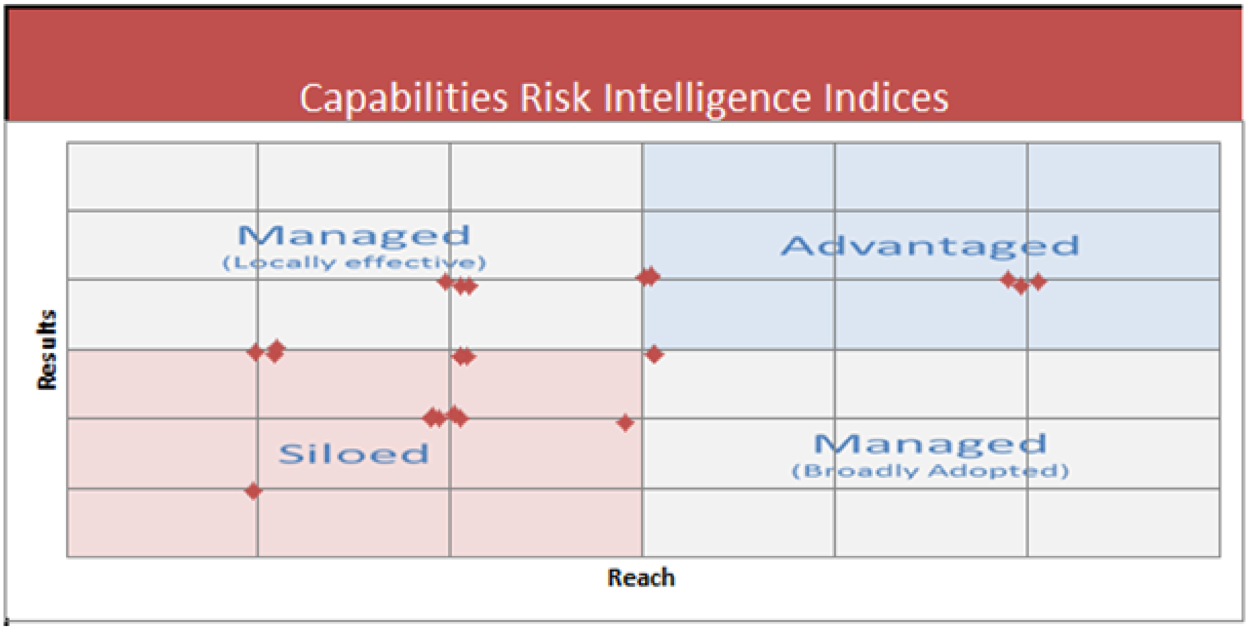
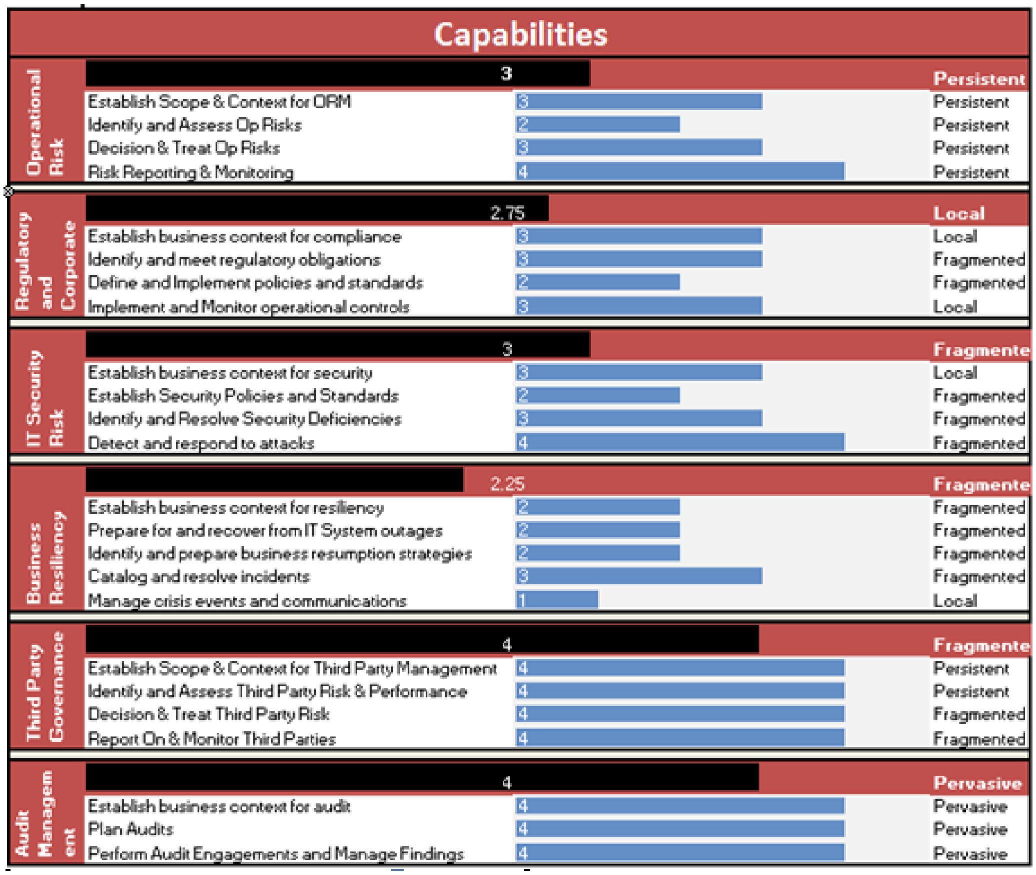


Figure 4. Domain Coverage

Capabilities

The Capabilities analysis includes the results of the different questions related to each dimension of Risk Intelligence. First, the Capabilities are clustered into the Risk Intelligence Index quadrants to give an overall analysis of enterprise capabilities. Next, key capabilities for each dimension are listed with the results based on the Risk Practices questions.





Capabilities			
Operational Risk		3	Persistent
	Establish Scope & Context for ORM	3	Persistent
	Identify and Assess Op Risks	2	Persistent
	Decision & Treat Op Risks	3	Persistent
	Risk Reporting & Monitoring	4	Persistent
Regulatory and Corporate		2.75	Local
	Establish business context for compliance	3	Local
	Identify and meet regulatory obligations	3	Fragmented
	Define and Implement policies and standards	2	Fragmented
	Implement and Monitor operational controls	3	Local
IT Security Risk		3	Fragmente
	Establish business context for security	3	Local
	Establish Security Policies and Standards	2	Fragmented
	Identify and Resolve Security Deficiencies	3	Fragmented
	Detect and respond to attacks	4	Fragmented
Business Resiliency		2.25	Fragmente
	Establish business context for resiliency	2	Fragmented
	Prepare for and recover from IT System outages	2	Fragmented
	Identify and prepare business resumption strategies	2	Fragmented
	Catalog and resolve incidents	3	Fragmented
	Manage crisis events and communications	1	Local
Third Party Governance		4	Fragmente
	Establish Scope & Context for Third Party Management	4	Persistent
	Identify and Assess Third Party Risk & Performance	4	Persistent
	Decision & Treat Third Party Risk	4	Fragmented
	Report On & Monitor Third Parties	4	Fragmented
Audit Managem ent		4	Pervasive
	Establish business context for audit	4	Pervasive
	Plan Audits	4	Pervasive
	Perform Audit Engagements and Manage Findings	4	Pervasive

This view gives an overview of the key capabilities needed within an organization to manage the six dimensions of Risk Intelligence, summaries the analysis of current practices and highlights areas of improvement.

CONCLUSION

The RSA Archer Risk Intelligence Index is a measurement of the overall maturity of the risk management practices within an organization. The assessment takes into consideration the organizational and environmental challenges of the organization to produce a Risk Challenge indicator. The Foundation of the organization's commitment to managing risk is assessed. Existing processes are assessed to measure the effectiveness and organizational reach of practices in six major dimensions of risk management. The results are indicators plotted into four major quadrants - Siloed, Managed (Locally Effective), Managed (Broadly Adopted) and Advantaged – giving insight into the areas of strengths and weakness within the existing risk strategy.

ABOUT THE RSA ARCHER MATURITY MODEL SERIES

RSA Archer's vision is to help organizations transform compliance, manage risk and exploit opportunity with Risk Intelligence made possible via an integrated, coordinated GRC program. The RSA Archer Maturity Model series of white papers outlines multiple segments of risk management that organizations must address to transform their GRC programs.

ABOUT RSA

RSA’s Intelligence Driven Security solutions help organizations reduce the risks of operating in a digital world. Through visibility, analysis, and action, RSA solutions give customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, prevent IP theft, fraud and cybercrime. For more information on RSA, please visit www.rsa.com.