LogicManager™

Presenting ERM to the Board

+1 617 530 1210 | logicmanager.com | info@logicmanager.com

Introduction

We know that risk managers are the heroes of their organizations. They, alongside their trusty ERM programs, empower their businesses to uphold their reputation, anticipate what's ahead, and improve business performance.

We also know that the Board can have a slightly different opinion of risk management. Some members might think that risk management takes too much time and attention away from other important business processes, or that the cost isn't worth the reward. It's your job, then, as risk managers to convince Board members that your programs are effective and worthwhile means to their ends.

Or perhaps your Board is already convinced that a robust ERM program is important; they just want more information about how effective it is and how it's helping them achieve their goals. As it happens, Board members are under more regulatory pressure than ever before to prove their organizations have effective risk management programs in place, which means they'll be looking to you for the reports to prove it.

No matter what kind of pressure you're under, whether it's lobbying for support or providing necessary reports, this eBook will give you the insight you need. We'll outline some goals you should set for your reports, take a look at some reports the Board will find particularly useful, and give you the steps you need to take to once and for all prove your heroism.

Table of Contents

2 Increased Need for ERM Reporting

5 Two Goals of Risk Management Reporting

8 Four Useful Presentations of Risk Information

18 How Do You Get Here?

23 The Future of ERM Board Reporting

Chapter 1

Increased Need for ERM Reporting

There are many factors that contribute to what we perceive as a drastic increase in the need for ERM reporting. We've already mentioned two: risk managers might need more support for their program, or Board members might be clamoring for more information.

Let's talk about some other contributing factors.

Measurable Value of ERM

There is now scientific evidence proving that organizations with a higher risk maturity have a stronger financial performance.

As one study states, “Firms that have successfully integrated the ERM process into both their strategic activities and everyday practices display superior ability in uncovering risk dependencies and correlations across the entire enterprise and, as a consequence, enhanced value when undertaking the ERM maturity journey.”

With this information out there, the Board needs reports and data that tell them exactly how much of this benefit they’re receiving.

Check out this blog!

Read more about how a mature ERM program increases your company’s market value. Read the blog to learn about the findings of this independent study.

Increased Pressure for ERM Reporting

Originally, Boards of Directors were only responsible for CEO-level of risk activities and decisions. Now, their accountability is extended down to the threshold of the material impact of risk, regardless of level. Risk now needs to be identified at the business process level where this material activity takes place.

Regulations such as this, along with court cases like Stone vs. Ridder that uphold them, now hold Board members personally responsible for risk management. Even private companies aren’t exempt, as this accountability extends to a company’s supply chain.

Ultimately, boards are now given a choice between having effective risk management, or disclosing their ineffectiveness to the public. If they do neither, it is considered fraud or negligence, as not knowing about a risk is no longer a viable defense.

Internal Audit’s New Role

Revisions to Internal Audit Standards Approved

- Changes to take effect January 2025
- Announced January 9, 2024

Internal Audit has been tasked with fact-checking the risk management information being presented to the Board in order to ensure its integrity from the business process activity level up.

In 2024, the Institute of Internal Auditors (IIA) announced changes to the IPPF which will be renamed Global Internal Audit Standards, effective Jan. 9, 2025.

These changes will help create a more simplified approach, increase transparency and participation with key stakeholders, support focus on current and emerging risks, and allow internal audits to take a risk-based approach to increase efficiency.

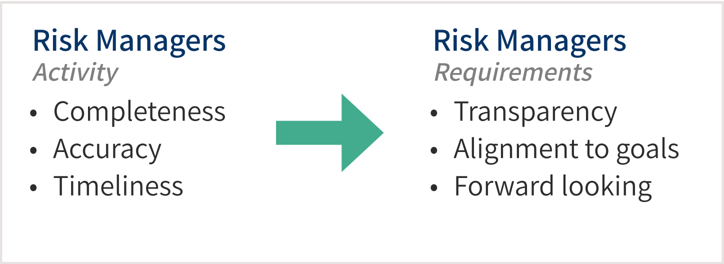
Responsibilities for Risk Managers

The role of the enterprise risk manager is clear: to close the gap between strategic level risk and all the operational risks occurring on the font lines of the organization. The risk manager is responsible for setting the standards, practices and procedures for effective risk management and embedding them in all existing business processes. In addition, the risk manager is now accountable for measuring the effectiveness of their ERM programs.

The latter requires putting a mechanism in place to collect risk-related information at the activity level, where most operational risks materialize, and aggregate this information in a format the Board cares about. While pursuing this task, the risk manager must also preserve the links between the information collected at the activity level and the resources associated with that information, so that the integrity trail is clear and useful for Internal Audit.

Board of Directors

- Risk Management oversight
- Make decisions on risk
- Ensure achievement of strategic imperatives



Risk Managers
Activity

- Completeness
- Accuracy
- Timeliness

Risk Managers
Requirements

- Transparency
- Alignment to goals
- Forward looking

Chapter 2

Two Goals of Risk Management Reporting

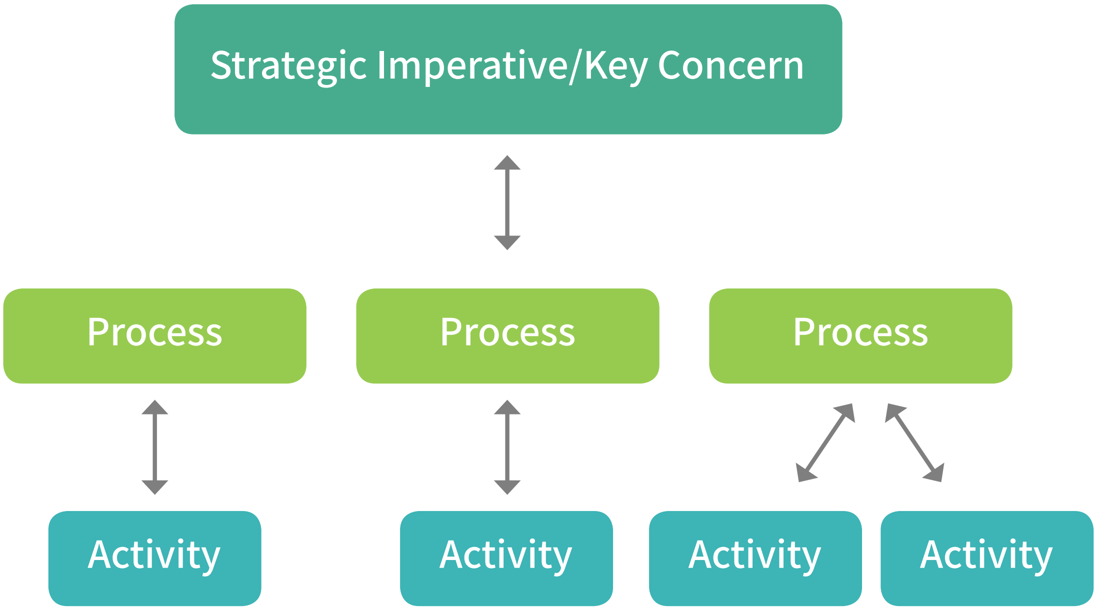
We believe performance is a direct result of effective risk management. The Board needs to believe this, too. The beauty of this belief is, with the right data collection and reporting techniques, it can be proven. The key to proving that risk management is instrumental to enhancing business performance is meeting the two goals of ERM reporting:

1. Alignment of risks and activities to strategic objectives and key concerns.
2. Demonstrable effectiveness of ERM.

Alignment of Risks and Activities to Strategic Objectives and Key Concerns

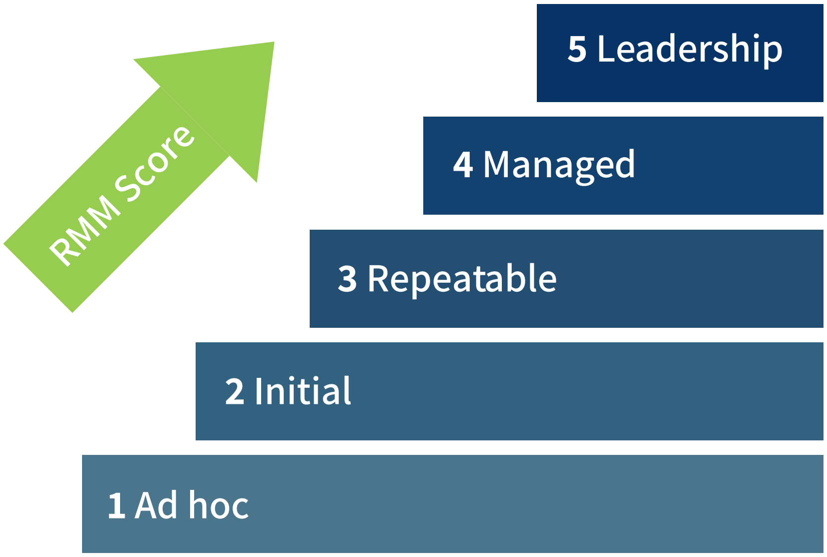
It goes without saying that a company's strategic goals are the utmost concern of the Board and senior executives. Getting an accurate pulse on strategic objectives is challenging, as these goals are cross-functional and event-based in nature, and taking action on these goals is impossible without operationalizing them.

This is where risk management comes in. The key is to break down these objectives into actionable, silo-specific activities within processes. When we understand which activities serve which processes, then we understand how these activities, and the risks related to them, impact strategic imperatives.



Effectiveness of ERM Efforts

ERM is a strategic process to gain competitive advantage through better decision-making, efficient deployment of scarce resources, and reduced exposure to negative events. As an organization’s risk management competency level improves, so does its ability to successfully manage various risks and achieve goals.



Remember the business value studies of ERM on page 3? This is why the board needs to know the effectiveness of your risk management program; they need to determine and measure how much of this valuation benefit the organization is getting.

Get Your Risk Maturity Score

The Risk Maturity Model (RMM) is a free online assessment tool that can benchmark the maturity of your ERM program. Take the free RMM assessment today!

Chapter 3

Four Useful Presentations of Risk Information

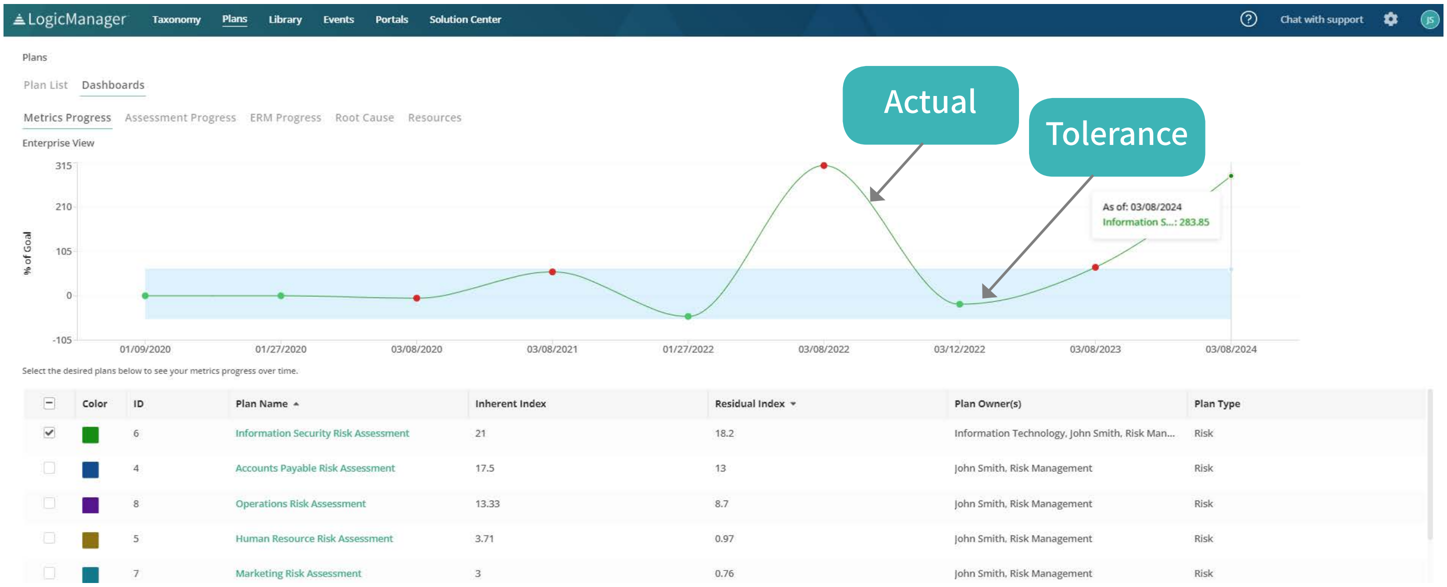
The truth is, risk management is hard stuff. We believe risk managers are the heroes of their organizations, in part, because they have a unique ability to not only understand a massive amount of data collected across business areas, but an ability to leverage this data to ensure top-of-the-line business performance.

Not everyone, however, has this gift. That's why it's up to you to present your findings in a way that is both relevant and interesting to your Board. Let's look at some presentations that accomplish just that.

Dashboard 1: Metrics Progress

Displays the development of risk tolerance over time.

Your organization's risk tolerance is an extremely valuable metric, as it can be used as a reference point that will help you visualize how your organization is handling its risk. Standardized risk assessments will enable you to first associate value and meaning with your risks, which will in turn help you determine your risk tolerance indexes over time. When you can measure your risks in a way that is relative to your organization's tolerance level, then you can prepare for, mitigate, and control risks before they fall out of tolerance. This type of view therefore makes it easy to show the Board which risks need to be prioritized.



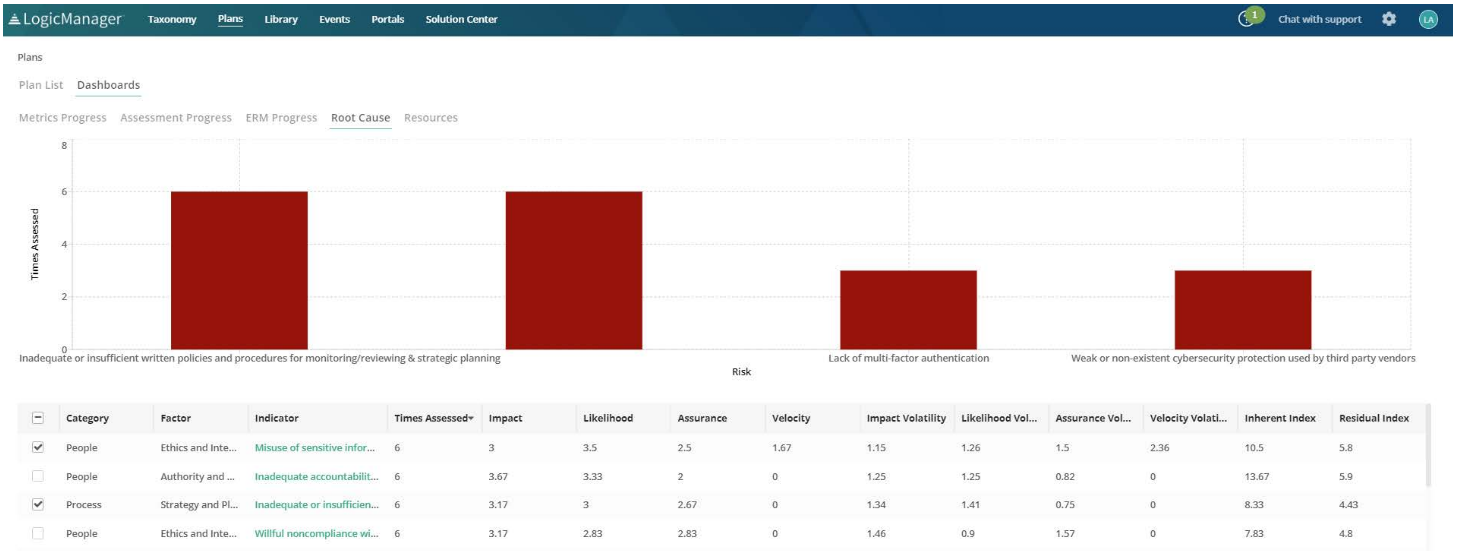
Select the desired plans below to see your metrics progress over time.

☐	Color	ID	Plan Name ▲	Inherent Index	Residual Index ▼	Plan Owner(s)	Plan Type
☑	🟩	6	Information Security Risk Assessment	21	18.2	Information Technology, John Smith, Risk Man...	Risk
☐	🟦	4	Accounts Payable Risk Assessment	17.5	13	John Smith, Risk Management	Risk
☐	🟪	8	Operations Risk Assessment	13.33	8.7	John Smith, Risk Management	Risk
☐	🟫	5	Human Resource Risk Assessment	3.71	0.97	John Smith, Risk Management	Risk
☐	🟦	7	Marketing Risk Assessment	3	0.76	John Smith, Risk Management	Risk

Dashboard 2: Root Cause

Offers an objective and transparent view across the organization.

Businesses are made up of many integral parts, which means it can be difficult to gain an enterprise-wide view of a company's risk, and therefore hard to know which risks are most pressing. This heat map shows all of an organization's risks in one view based on highly accurate activity-level observations. Issues that fall on the upper right corner, for instance, are the most critical, and therefore deserve more resources. This information also stays current, as any changes in assessments are immediately reflected.

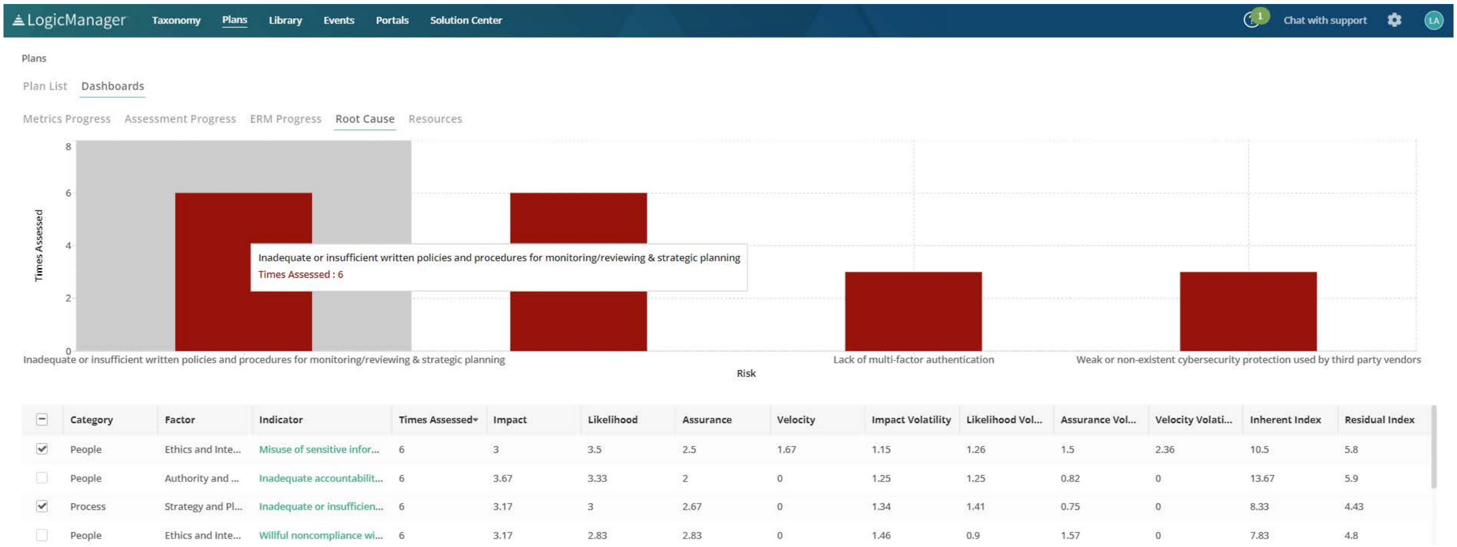

LogicManager
Taxonomy
Plans
Library
Events
Portals
Solution Center
1
Chat with support
LA
Plans
Plan List
Dashboards
Metrics Progress
Assessment Progress
ERM Progress
Root Cause
Resources
Times Assessed
8
6
4
2
0
Inadequate or insufficient written policies and procedures for monitoring/reviewing & strategic planning
Lack of multi-factor authentication
Weak or non-existent cybersecurity protection used by third party vendors
Risk

⊟	Category	Factor	Indicator	Times Assessed▾	Impact	Likelihood	Assurance	Velocity	Impact Volatility	Likelihood Vol...	Assurance Vol...	Velocity Volati...	Inherent Index	Residual Index
☑	People	Ethics and Inte...	Misuse of sensitive infor...	6	3	3.5	2.5	1.67	1.15	1.26	1.5	2.36	10.5	5.8
□	People	Authority and ...	Inadequate accountabilit...	6	3.67	3.33	2	0	1.25	1.25	0.82	0	13.67	5.9
☑	Process	Strategy and Pl...	Inadequate or insufficien...	6	3.17	3	2.67	0	1.34	1.41	0.75	0	8.33	4.43
□	People	Ethics and Inte...	Willful noncompliance wi...	6	3.17	2.83	2.83	0	1.46	0.9	1.57	0	7.83	4.8

Example Root Cause Dashboard

Reporting by Strategic Imperative

Oftentimes, the root cause of an issue cannot be determined by looking at one area of the business. ERM programs are designed to leverage information assessed across multiple silos and levels of the organization, and to see the connections between risks across silos, so that the root cause of a risk can be determined and mitigated. With this dashboard, you can also view risk by a theme, like an initiative or key concern. This can enable organizations to move forward on an initiative because it gives them all the information concerning the risks, opportunities, and accountability associated with the initiative. That's how better decisions are made.


LogicManager
Taxonomy
Plans
Library
Events
Portals
Solution Center
1
Chat with support
LA
Plans
Plan List
Dashboards
Metrics Progress
Assessment Progress
ERM Progress
Root Cause
Resources
8
6
4
2
0
Times Assessed
Inadequate or insufficient written policies and procedures for monitoring/reviewing & strategic planning
Times Assessed : 6
Inadequate or insufficient written policies and procedures for monitoring/reviewing & strategic planning
Lack of multi-factor authentication
Weak or non-existent cybersecurity protection used by third party vendors
Risk

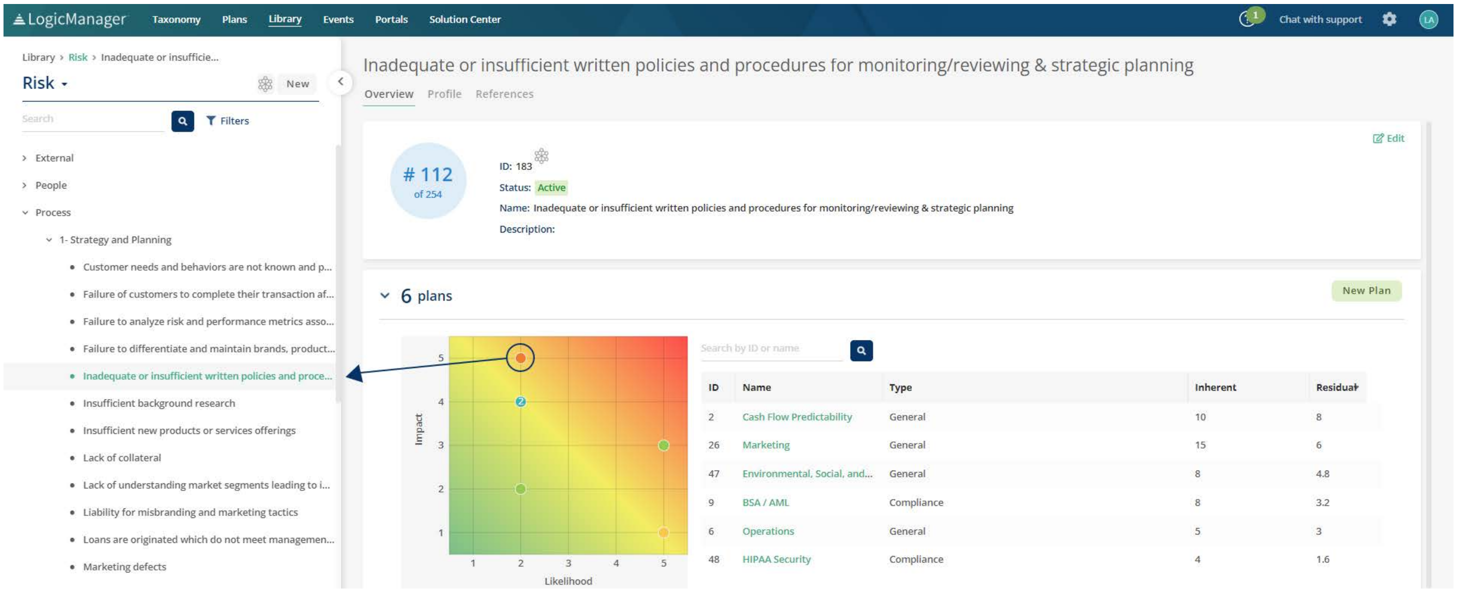
⊟	Category	Factor	Indicator	Times Assessed▾	Impact	Likelihood	Assurance	Velocity	Impact Volatility	Likelihood Vol...	Assurance Vol...	Velocity Volati...	Inherent Index	Residual Index
☑	People	Ethics and Inte...	Misuse of sensitive infor...	6	3	3.5	2.5	1.67	1.15	1.26	1.5	2.36	10.5	5.8
□	People	Authority and ...	Inadequate accountabilit...	6	3.67	3.33	2	0	1.25	1.25	0.82	0	13.67	5.9
☑	Process	Strategy and Pl...	Inadequate or insufficien...	6	3.17	3	2.67	0	1.34	1.41	0.75	0	8.33	4.43
□	People	Ethics and Inte...	Willful noncompliance wi...	6	3.17	2.83	2.83	0	1.46	0.9	1.57	0	7.83	4.8

Example Root Cause Dashboard

Reporting by Strategic Imperative - Cash Flow Predictability

Risk managers often need to provide more detailed, underlying data for risks that affect strategic goals, such as which business areas are involved in achieving such a goal, a goal's individual risk profile, and what mitigation and monitoring strategies are in place. By leveraging your risk taxonomy, you can easily pull up that information and create more granular dashboards for strategic objectives, like "Cash Flow Predictability."

In this example, the risk manager can clearly see that although several risks are identified for Cash Flow Predictability, the current "failure to analyze risk and performance metrics associated with strategy" should be her top priority. It has a higher inherent risk, as displayed by its plot position in the upper right corner, as well as a higher residual index score, as shown in the table. With an understanding of the key risk factor, she can determine a key mitigation activity.



- External
- People
- Process
  - 1- Strategy and Planning
    - Customer needs and behaviors are not known and p...
    - Failure of customers to complete their transaction af...
    - Failure to analyze risk and performance metrics asso...
    - Failure to differentiate and maintain brands, product...
    - Inadequate or insufficient written policies and proce...
    - Insufficient background research
    - Insufficient new products or services offerings
    - Lack of collateral
    - Lack of understanding market segments leading to i...
    - Liability for misbranding and marketing tactics
    - Loans are originated which do not meet managemen...
    - Marketing defects

Inadequate or insufficient written policies and procedures for monitoring/reviewing & strategic planning

112 of 254

ID: 183
Status: Active
Name: Inadequate or insufficient written policies and procedures for monitoring/reviewing & strategic planning
Description:

6 plans

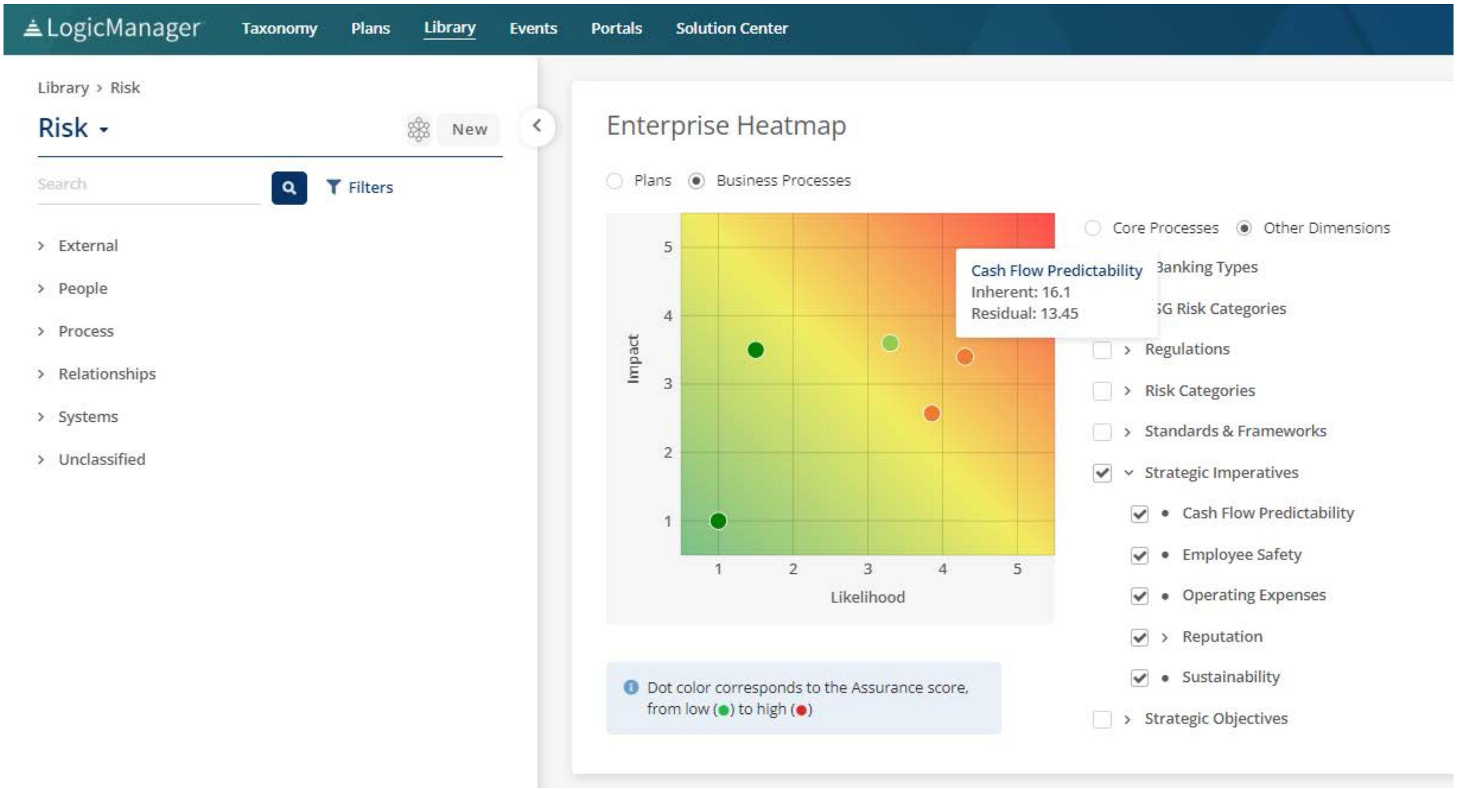
ID	Name	Type	Inherent	Residual
2	Cash Flow Predictability	General	10	8
26	Marketing	General	15	6
47	Environmental, Social, and...	General	8	4.8
9	BSA / AML	Compliance	8	3.2
6	Operations	General	5	3
48	HIPAA Security	Compliance	4	1.6

Dashboard 3: Enterprise View

Organizes information by strategic imperative

The risk manager should be able to drill down on the risks related to strategic objectives. This allows her to present an aggregation of risks organized by the strategic imperative they relate to. As we've said, strategic objectives are what matters to your Board. This dashboard allows you to put risk in a context that senior executives truly care about.

This dashboard is also a great example of making your reports actionable. Your Board will be able to easily identify which business areas contribute to a certain objective, what the root cause issues are, and where resources should be allocated.



○ Plans ● Business Processes

○ Core Processes ● Other Dimensions

Cash Flow Predictability
Inherent: 16.1
Residual: 13.45

- Banking Types
- ESG Risk Categories
- □ › Regulations
- □ › Risk Categories
- □ › Standards & Frameworks
- ☑ ⌄ Strategic Imperatives
  - ☑ • Cash Flow Predictability
  - ☑ • Employee Safety
  - ☑ • Operating Expenses
  - ☑ › Reputation
  - ☑ • Sustainability
- □ › Strategic Objectives

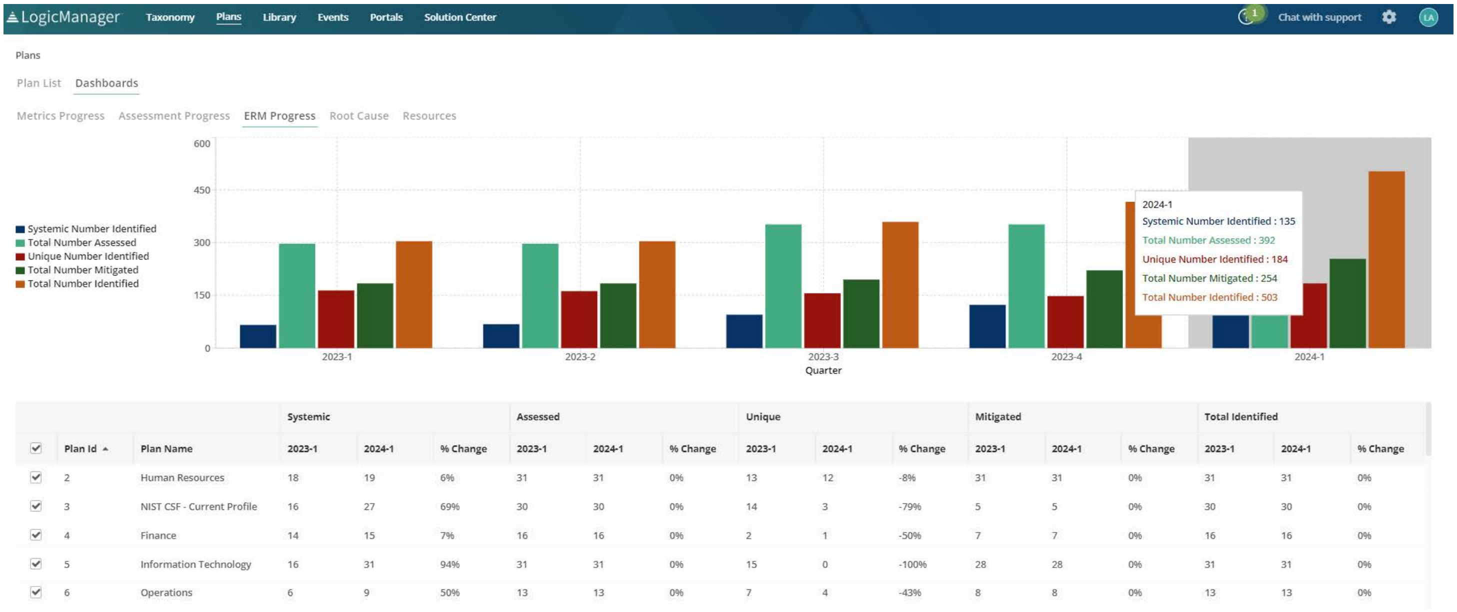
Dot color corresponds to the Assurance score, from low (🟢) to high (🔴)

Dashboard 4: ERM Progress

Measures the effectiveness of your ERM program

As we mentioned earlier, a risk manager’s presentation to the Board should be two-fold. Fold one: demonstrate how risks across the organization will roll-up to impact the Board’s strategic objectives and key concerns, which we’ve covered. Fold two: provide key measures that validate and track the progress of the ERM program. The following are examples of measures that will quantify the value your ERM program is providing.

ERM is cross-functional in nature, and cannot be done in silos. Process owners own the risk and risk managers own the completeness, timeliness, and accuracy of the risk information. The more process owners are involved in risk assessments, the more accurate and forward-looking the information collected will be. Both attributes, accurate and forward-looking, are extremely valuable qualities of information to the organization.



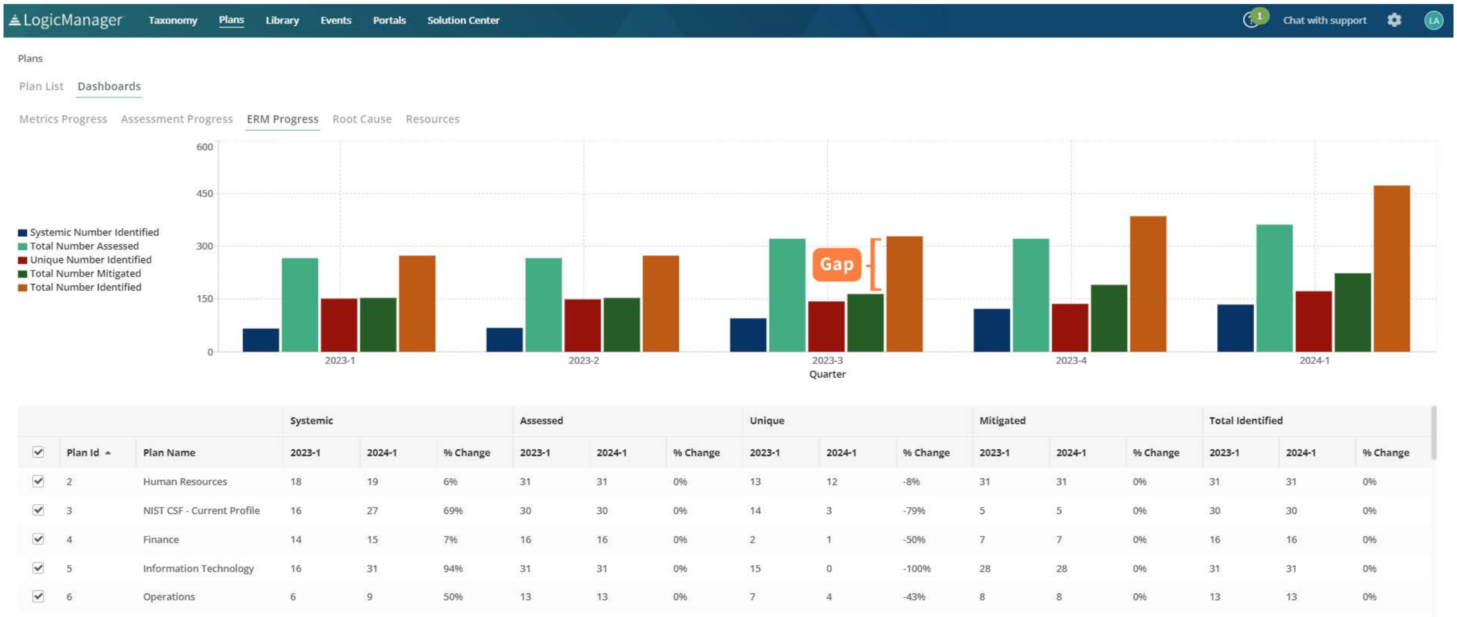
			Systemic			Assessed			Unique			Mitigated			Total Identified		
☑	Plan Id ▲	Plan Name	2023-1	2024-1	% Change	2023-1	2024-1	% Change	2023-1	2024-1	% Change	2023-1	2024-1	% Change	2023-1	2024-1	% Change
☑	2	Human Resources	18	19	6%	31	31	0%	13	12	-8%	31	31	0%	31	31	0%
☑	3	NIST CSF - Current Profile	16	27	69%	30	30	0%	14	3	-79%	5	5	0%	30	30	0%
☑	4	Finance	14	15	7%	16	16	0%	2	1	-50%	7	7	0%	16	16	0%
☑	5	Information Technology	16	31	94%	31	31	0%	15	0	-100%	28	28	0%	31	31	0%
☑	6	Operations	6	9	50%	13	13	0%	7	4	-43%	8	8	0%	13	13	0%

Example ERM Progress Dashboard

Reporting by the total number of risks identified and mitigated

In the graph below, the red bar shows the number of risks identified and assessed for each business process or business area. These bars tell the Board how many of the risks in the enterprise have been uncovered and evaluated.

But risk management doesn't stop at risk identification and assessment. It's critical to show the Board how many of those risks are also covered by mitigation activities. Notice the gap between the red bar measuring the number of risks identified and assessed, and the green bar measuring the number covered by mitigation activities. See how the gap is getting smaller quarter by quarter? This is the best way to show both the current state of your ERM program, and how it has progresses over the past several quarters.



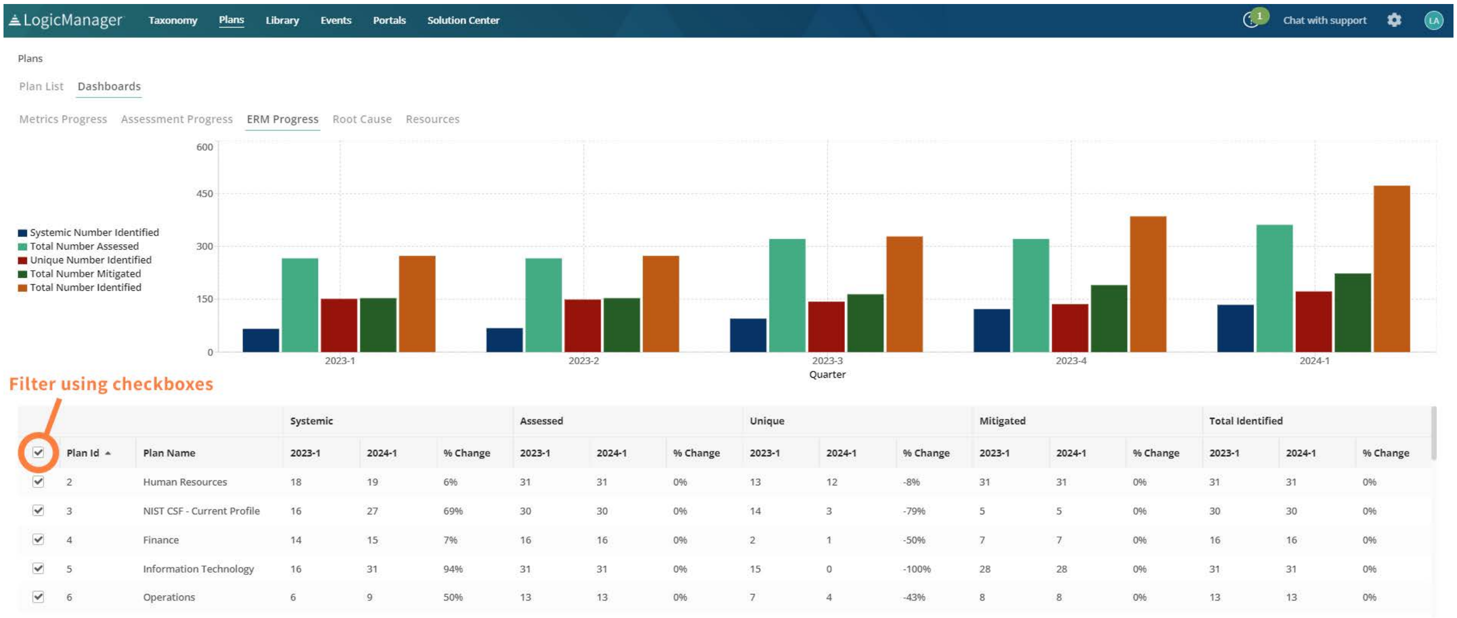
			Systemic			Assessed			Unique			Mitigated			Total Identified		
☑	Plan Id ▲	Plan Name	2023-1	2024-1	% Change	2023-1	2024-1	% Change	2023-1	2024-1	% Change	2023-1	2024-1	% Change	2023-1	2024-1	% Change
☑	2	Human Resources	18	19	6%	31	31	0%	13	12	-8%	31	31	0%	31	31	0%
☑	3	NIST CSF - Current Profile	16	27	69%	30	30	0%	14	3	-79%	5	5	0%	30	30	0%
☑	4	Finance	14	15	7%	16	16	0%	2	1	-50%	7	7	0%	16	16	0%
☑	5	Information Technology	16	31	94%	31	31	0%	15	0	-100%	28	28	0%	31	31	0%
☑	6	Operations	6	9	50%	13	13	0%	7	4	-43%	8	8	0%	13	13	0%

Example ERM Progress Dashboard

Reporting by cut levels

Having a sense of your overall risk coverage is important. But what's even more valuable is knowing if your organization's key risks are covered. You can use your organization's risk tolerance to prioritize the allocation of resources to the risks that need stronger coverage, rather than wasting resources on risks that will have no major impact on your organization. Performing a gap analysis with a tolerance level will also help you to identify emerging risks as they rise out of tolerance, which will signal that some mitigation activities in place are no longer sufficient.

In this view, you can also filter out low risks, and focus on above average risk. This way, you can easily show the board the risks and the corresponding mitigation activities that directly impact each of the organization's corporate objectives and business performance.



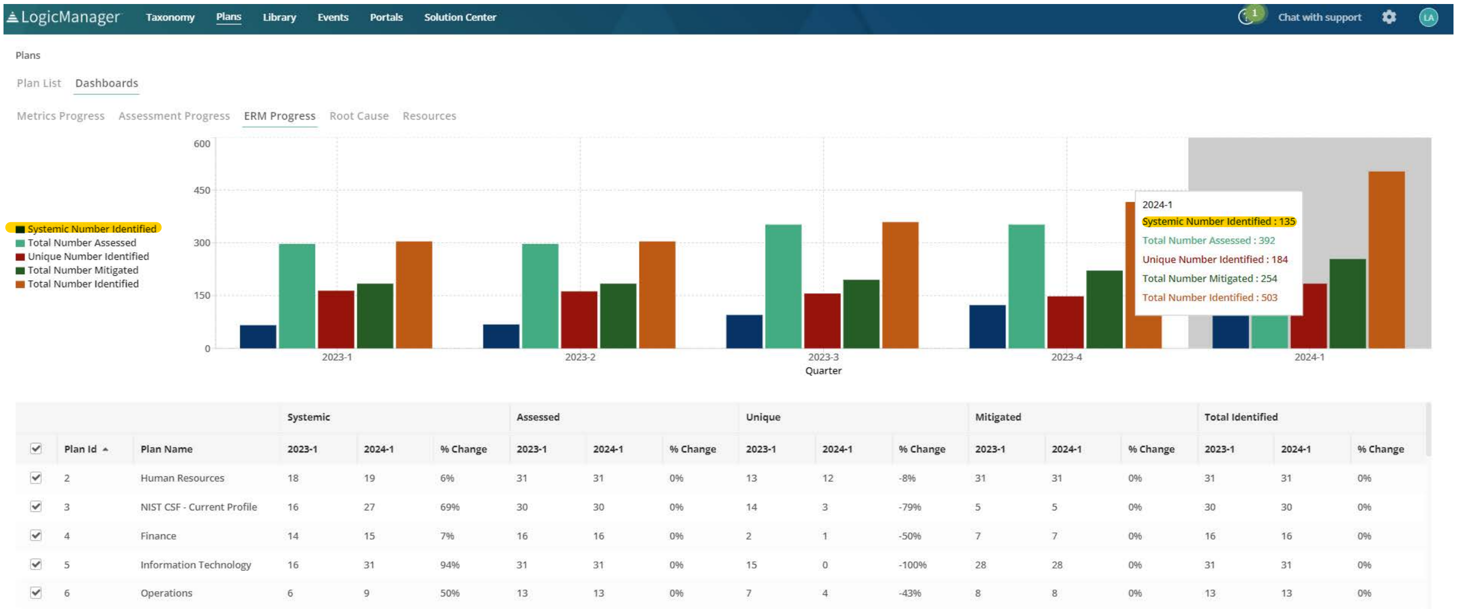
Filter using checkboxes

			Systemic			Assessed			Unique			Mitigated			Total Identified		
☑	Plan Id ▲	Plan Name	2023-1	2024-1	% Change	2023-1	2024-1	% Change	2023-1	2024-1	% Change	2023-1	2024-1	% Change	2023-1	2024-1	% Change
☑	2	Human Resources	18	19	6%	31	31	0%	13	12	-8%	31	31	0%	31	31	0%
☑	3	NIST CSF - Current Profile	16	27	69%	30	30	0%	14	3	-79%	5	5	0%	30	30	0%
☑	4	Finance	14	15	7%	16	16	0%	2	1	-50%	7	7	0%	16	16	0%
☑	5	Information Technology	16	31	94%	31	31	0%	15	0	-100%	28	28	0%	31	31	0%
☑	6	Operations	6	9	50%	13	13	0%	7	4	-43%	8	8	0%	13	13	0%

Example ERM Progress Dashboard

Reporting by systemic risk

Overtime, you will be able to add other measures to your Board presentations, such as the alignment of risks across business silos. This is known as systemic risk identification. The blue bar shows the detection of upstream and downstream dependencies throughout your organization, that is, when one area of the organization is unknowingly causing strain on other areas. A huge benefit of this view is that you will now know which business areas would benefit from centralized controls, as opposed to controls assigned specifically to one business area. By assigning one control that will simultaneously mitigate risk in many business areas, you can drastically reduce the extra time and money of maintaining separate activity-level controls.



			Systemic			Assessed			Unique			Mitigated			Total Identified		
☑	Plan Id ▲	Plan Name	2023-1	2024-1	% Change	2023-1	2024-1	% Change	2023-1	2024-1	% Change	2023-1	2024-1	% Change	2023-1	2024-1	% Change
☑	2	Human Resources	18	19	6%	31	31	0%	13	12	-8%	31	31	0%	31	31	0%
☑	3	NIST CSF - Current Profile	16	27	69%	30	30	0%	14	3	-79%	5	5	0%	30	30	0%
☑	4	Finance	14	15	7%	16	16	0%	2	1	-50%	7	7	0%	16	16	0%
☑	5	Information Technology	16	31	94%	31	31	0%	15	0	-100%	28	28	0%	31	31	0%
☑	6	Operations	6	9	50%	13	13	0%	7	4	-43%	8	8	0%	13	13	0%

Chapter 4

How Do You Get Here?

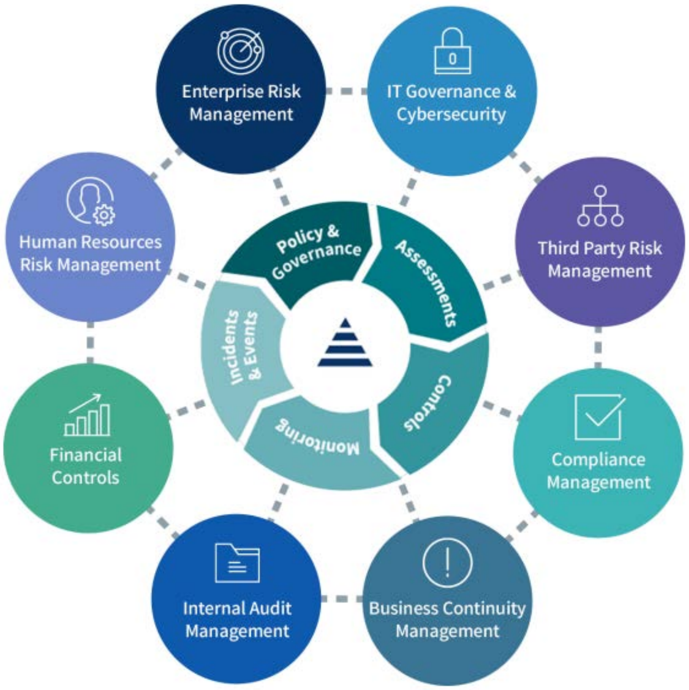
The challenge is assembling information across functions and levels, while keeping one comprehensible picture of risk for the Board. How do you currently quantify your organization's risks? Are you able to link operational risks to the strategic goals they impact?

These are the questions we most often find risk managers struggling with when trying to provide their Board the information they want and need.

Risk Taxonomy is the Solution

To overcome the challenge of providing a comprehensive view of the organization's risks that accounts for all business areas, organizations need to build a robust risk taxonomy. Risk taxonomy is the practice and science of naming, classifying, and defining relationships between resources, risks, goals and business processes in the enterprise.

Once information is structured and the relationships within your organization are explicit, then assessments of this information can be carried out on the same standards and assumptions. Standardizing your risk assessments in this way makes the information you collect comparable, which means it can be utilized cross-functionally for more accurate and actionable risk management.


Enterprise Risk Management
IT Governance & Cybersecurity
Human Resources Risk Management
Third Party Risk Management
Financial Controls
Compliance Management
Internal Audit Management
Business Continuity Management
Policy & Governance
Assessments
Controls
Monitoring
Incidents & Events

Integrate Your Governance Areas

Check out our ebook, How to Integrate Risk and Governance Areas. We'll walk you through the process of building a standardized risk governance structure.

Step 1. Take a Root-Cause Approach

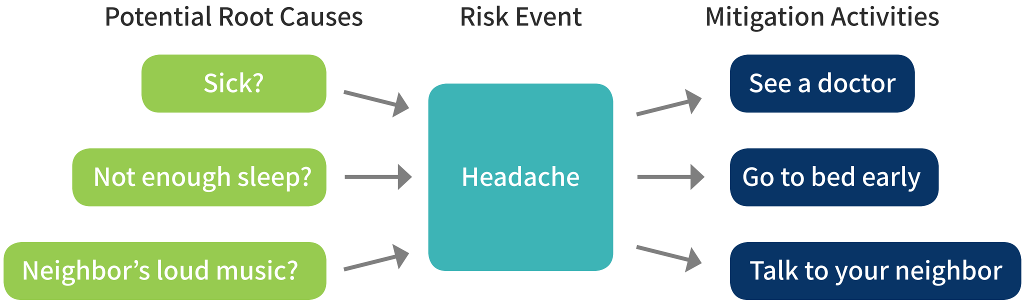
Risk managers should provide a **common root cause risk indicator library** to process owners so that systemic risks as well as upstream and downstream dependencies can be easily identified and mitigated. When every process owner is speaking the same risk language, then the answers they provide on risk assessments are comparable across business areas.

If multiple process owners choose the same root cause risk indicator, then the risk manager will know that this root cause is systemic, or that there is a potential dependency to be uncovered. As we've said, this method also uncovers areas that would benefit from centralized controls, which eliminates the extra work of maintaining activity-specific controls.

The most effective way to collect risk data is to identify risk by root cause. Root cause tells us why an event occurs. Identifying the root cause of a risk tells us exactly what triggers a loss and where an organization is vulnerable. Only after the root cause is identified can you then apply effective mitigation tactics.

Example:

Let's look at a simple example to demonstrate this point. A risk event may be that you have a headache.



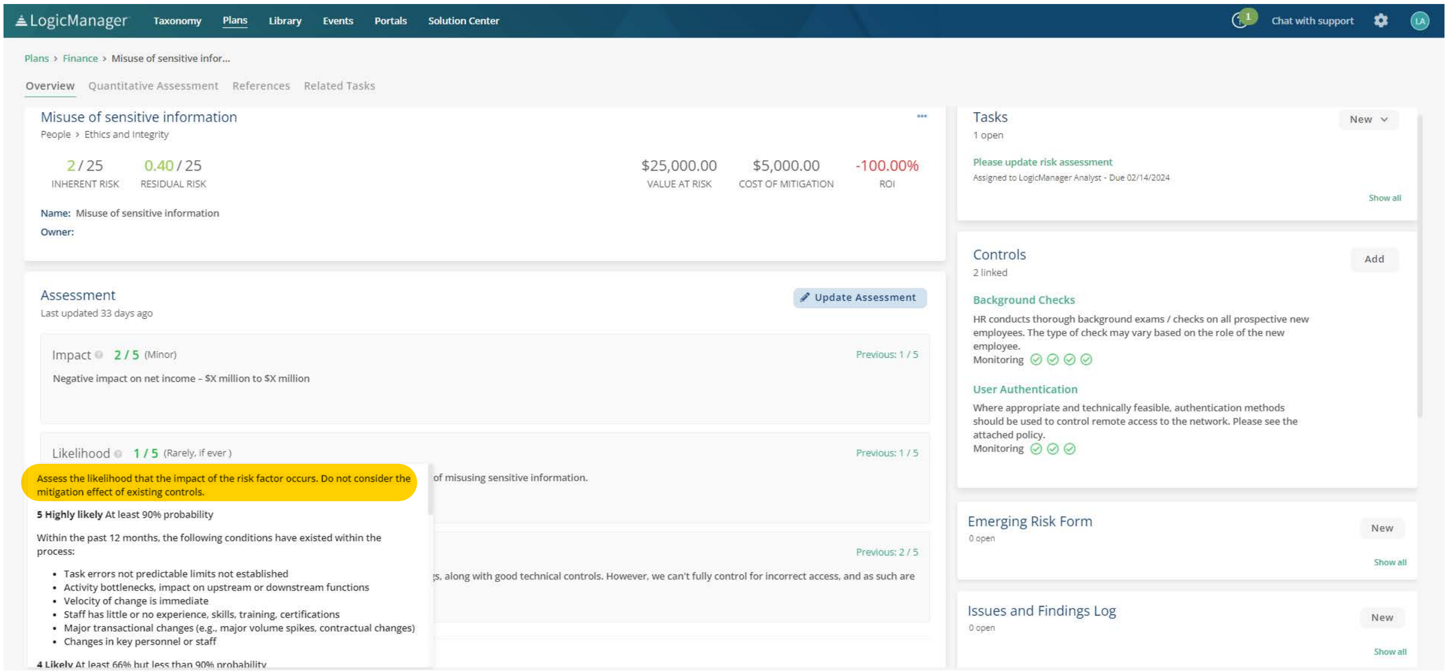
In order to cure a headache, we need to know why we have one. Armed with the knowledge of the source of a risk, we can proactively manage risk and avoid future risk events.

Mitigation activities need to be aimed at root cause, and will differ depending on the source of risk. In this example, it is easy to see why creating mitigation activities aimed at the risk event, rather than the root cause, can lead to very ineffective mitigation. If you take medicine to cure your headache when the true cause was lack of sleep, then you'll still have a headache when the medicine wears off.

What the BOD and senior management know is that they want to avoid headaches. Your responsibility as a risk manager is to determine what the potential root-causes of these headaches are so that appropriate mitigation activities can be employed.

Step 2. Standardize Assessment Scale and Criteria

The key is to standardize your risk assessments. All assessments should be standardized with a common numerical scale and criteria. When assessments are carried out on the same standards and assumptions, they become objective, quantifiable, repeatable, and comparable. They can be utilized cross-functionally, which enables better analysis, issue resolution, and issue escalation when necessary.



Misuse of sensitive information

People › Ethics and Integrity

2 / 25 INHERENT RISK · 0.40 / 25 RESIDUAL RISK · $25,000.00 VALUE AT RISK · $5,000.00 COST OF MITIGATION · -100.00% ROI

Name: Misuse of sensitive information

Owner:

Assessment

Last updated 33 days ago

Impact 2 / 5 (Minor) — Previous: 1 / 5

Negative impact on net income – $X million to $X million

Likelihood 1 / 5 (Rarely, if ever) — Previous: 1 / 5

of misusing sensitive information.

Previous: 2 / 5

;s, along with good technical controls. However, we can't fully control for incorrect access, and as such are

Assess the likelihood that the impact of the risk factor occurs. Do not consider the mitigation effect of existing controls.

5 Highly likely At least 90% probability

Within the past 12 months, the following conditions have existed within the process:

- Task errors not predictable limits not established
- Activity bottlenecks, impact on upstream or downstream functions
- Velocity of change is immediate
- Staff has little or no experience, skills, training, certifications
- Major transactional changes (e.g., major volume spikes, contractual changes)
- Changes in key personnel or staff

4 Likely At least 66% but less than 90% probability

Tasks

1 open

Please update risk assessment

Assigned to LogicManager Analyst - Due 02/14/2024

Controls

2 linked

Background Checks

HR conducts thorough background exams / checks on all prospective new employees. The type of check may vary based on the role of the new employee.

Monitoring ✓ ✓ ✓ ✓

User Authentication

Where appropriate and technically feasible, authentication methods should be used to control remote access to the network. Please see the attached policy.

Monitoring ✓ ✓ ✓

Emerging Risk Form

0 open

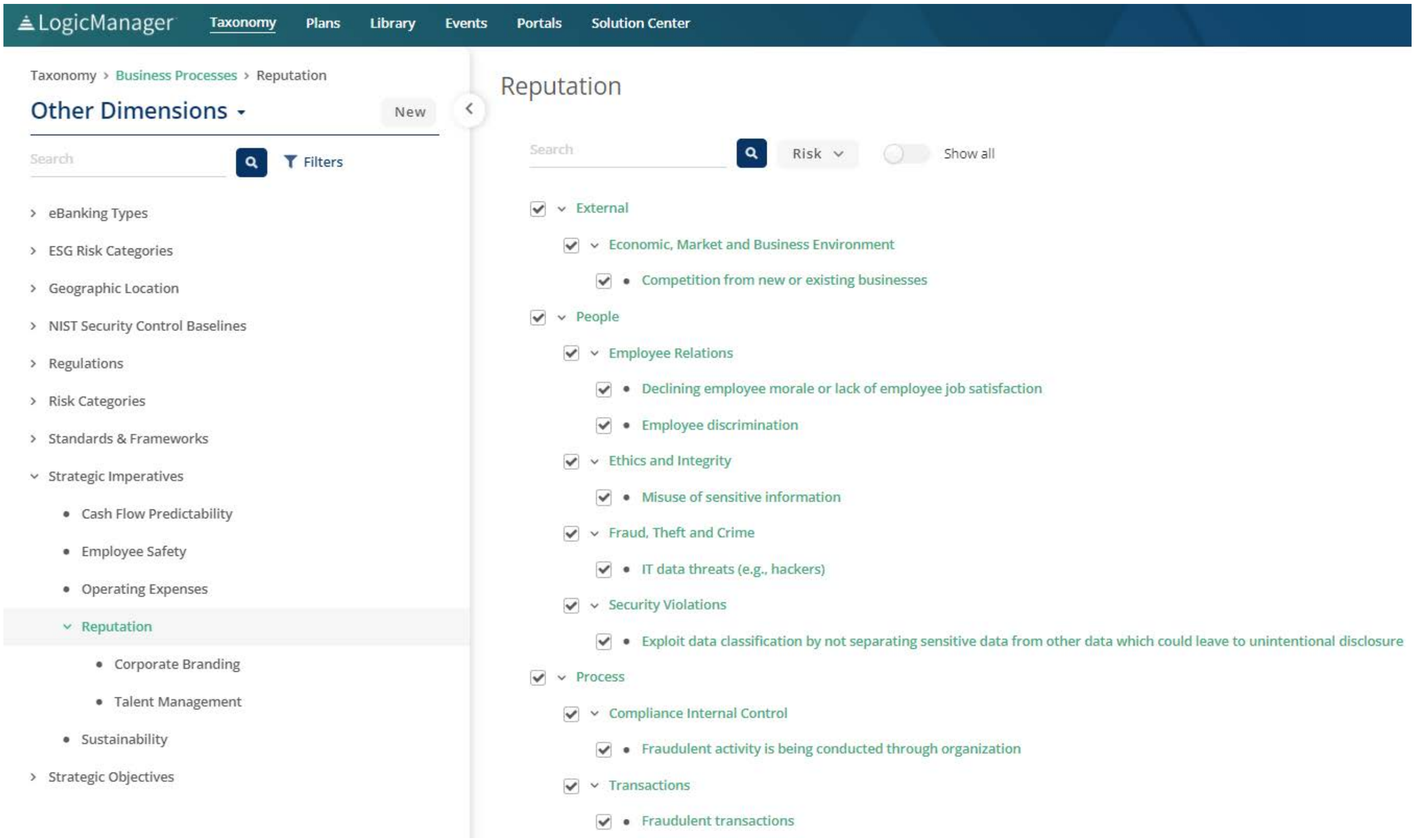
Issues and Findings Log

0 open

Step 3. Align Risks, Activities, and Goals

The Board of Directors and senior management know the outcomes they want to achieve and avoid. Your responsibility as a risk manager is to determine what the root causes of these outcomes are and how to best address them.

We can't stress this enough: you need to connect root-cause risks to corporate goals. You can find your organization's strategic goals from strategic plans and other places within your organization. The next step is to identify a number of root cause risks that could threaten to derail these corporate goals. Next, work with different business areas and process owners to understand which strategic goals their specific activities connect to. You can then align the risks you've identified with the activities you now understand to be connected with certain strategic objectives. Now you have a linear alignment of risk, activity, and goal.



Taxonomy › Business Processes › Reputation

Other Dimensions

- eBanking Types
- ESG Risk Categories
- Geographic Location
- NIST Security Control Baselines
- Regulations
- Risk Categories
- Standards & Frameworks
- Strategic Imperatives
  - Cash Flow Predictability
  - Employee Safety
  - Operating Expenses
  - Reputation
    - Corporate Branding
    - Talent Management
  - Sustainability
- Strategic Objectives

Reputation

- ☑ External
  - ☑ Economic, Market and Business Environment
    - ☑ Competition from new or existing businesses
- ☑ People
  - ☑ Employee Relations
    - ☑ Declining employee morale or lack of employee job satisfaction
    - ☑ Employee discrimination
  - ☑ Ethics and Integrity
    - ☑ Misuse of sensitive information
  - ☑ Fraud, Theft and Crime
    - ☑ IT data threats (e.g., hackers)
  - ☑ Security Violations
    - ☑ Exploit data classification by not separating sensitive data from other data which could leave to unintentional disclosure
- ☑ Process
  - ☑ Compliance Internal Control
    - ☑ Fraudulent activity is being conducted through organization
  - ☑ Transactions
    - ☑ Fraudulent transactions

Chapter 5

The Future of ERM Board Reporting

Now that we've covered the goals your presentations should accomplish, the data your reports should contain, and how you should be collecting this information, let's take a look at the direction ERM board reporting is going to take.

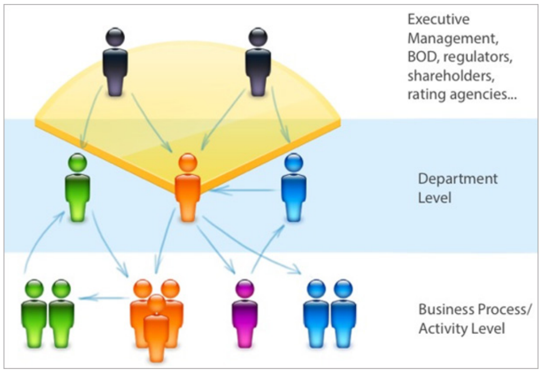
Ultimately, you will find that the insights we've given you will place your reporting techniques ahead of the curve. Just another reason to call yourself a hero.

Three Key Insights to ERM Board Reporting

1

Risk Disclosures

Instead of 10K and 10Q risk disclosures being isolated legal and compliance processes that are merely defensible risks lacking context, these disclosures will actually need to make the connection to the activity level.

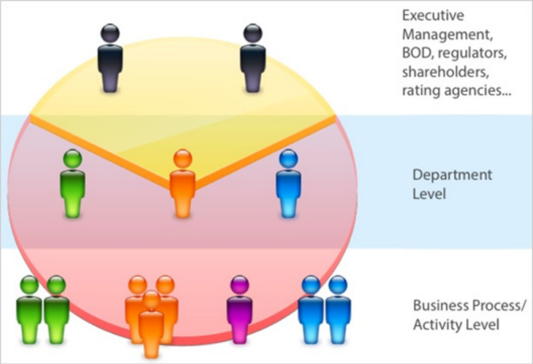

Executive Management, BOD, regulators, shareholders, rating agencies...
Department Level
Business Process/ Activity Level

2

Connection to Activities

Regulators are going to say, “Show me your disclosures on risk and show me how they connect to actual procedures and activities you’ve put in place to control them at the business process activity level.” What does this mean?

You will need to show how your disclosures have been operationalized: what business area do they stem from, who’s accountable for these risks, and what mitigation activities are being implemented.

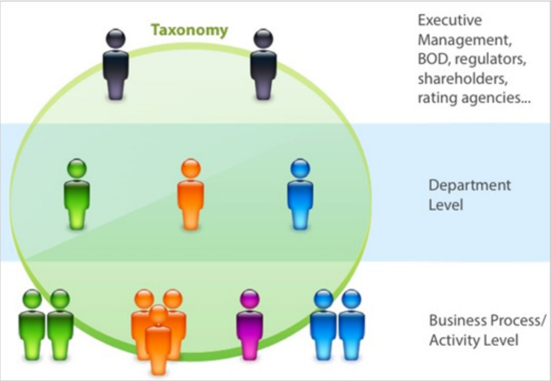

Executive Management, BOD, regulators, shareholders, rating agencies...
Department Level
Business Process/ Activity Level

3

Top-Down and Bottom-Up

Yes, the strategic goals your Board sets, the actions senior executives take, and the laws regulators enforce are all important. But it can’t be an entirely top-down approach.

Most risk events stem from the front lines, so you’ve got to be picking up on things that are happening at the activity level. The more process owners involved, the more accurate the information you’re collecting is, and the more prepared you are to mitigate risk.


Taxonomy
Executive Management, BOD, regulators, shareholders, rating agencies...
Department Level
Business Process/ Activity Level

LogicManager Can Help Your Business Present to the Board

Speak with one of our risk experts to learn how our enterprise risk management software empowers organizations to uphold their reputation, anticipate what's ahead, and improve business performance.

REQUEST A DEMO

INTERNAL AUDIT MANAGEMENT

BUSINESS CONTINUITY & DR

COMPLIANCE MANAGEMENT

HR RISK MANAGEMENT

ENTERPRISE RISK MANAGEMENT

FINANCIAL CONTROLS (SOX, MAR)

POLICY MANAGEMENT

THIRD PARTY RISK MANAGEMENT

IT GOVERNANCE & SECURITY

+1 617 530 1210 | logicmanager.com | info@logicmanager.com