RadarFirst

Build Risk Reporting Maturity

A STEP-BY-STEP WORKBOOK TO HELP COMMUNICATE VALUE AND DEMONSTRATE EFFECTIVENESS TO STAKEHOLDERS

How to Use This Guide

This guide will help put together your risk metrics to tell your data story, communicating your program value with your organization's goals and where it needs to improve. You will learn how to:

1. Identify Your Process in the Incident Management Cycle
2. Assess Your Organization's Maturity Level
3. Identify Your Audience
4. Tell the Data Story

Plan on reading and going back to different sections as you evolve your reporting processes and risk program's activities.

Contents

Introduction to Risk Reporting

Why Report on Risk?

Quality risk reporting forms the bedrock of a well-run program handling organizational compliance. Without this foundation, organizations risk insufficient resources and capabilities to manage the increasing number of threats that occur across departments.

To remediate, notify, and prevent critical risks, businesses must know what resources they have, what they need, why, and how to use existing assets. Organizations get this reliable information from useful metrics and an understanding of the context around them.

By putting valuable measurements together with a data story — an explanation of how the initiative meets organizational goals — risk reporting drives companies towards a higher ROI of their risk management programs and show what these initiatives have already achieved.

Risk Reporting Purposes

Informing a Specific Audience: Creating meaningful dialogues when explaining metrics and what you're doing about them.

Improving Risk Program Efficiency: Defining the maturity of a reporting program in its current form and how it could get better in the next one, three, or five years.

Informing Organization-Wide Training: Identifying lines of business, departments, or individuals who have disclosed or risk disclosing personal information and assigning training to them.

Factors Impacting Risk Reporting

Telling good data stories and meeting reporting objectives first requires understanding the factors impacting reporting. These components show where to focus reporting processes and content.

Process Steps in Incident Management

Risk leaders must prepare reports while simultaneously managing risk. Identifying where you are in this process helps ensure you separate information gathering from available information.

Maturity

Maturity describes the data-driven readiness of an organization to identify and escalate incidents quickly to resolve them as soon as possible. How you assess your organization depends on how you interpret the metrics.

Audience

Knowing the audience helps you best communicate and quantify your risk metrics in the report. That way, you get your listeners and readers engaged and ready for the next activity to reduce risks.

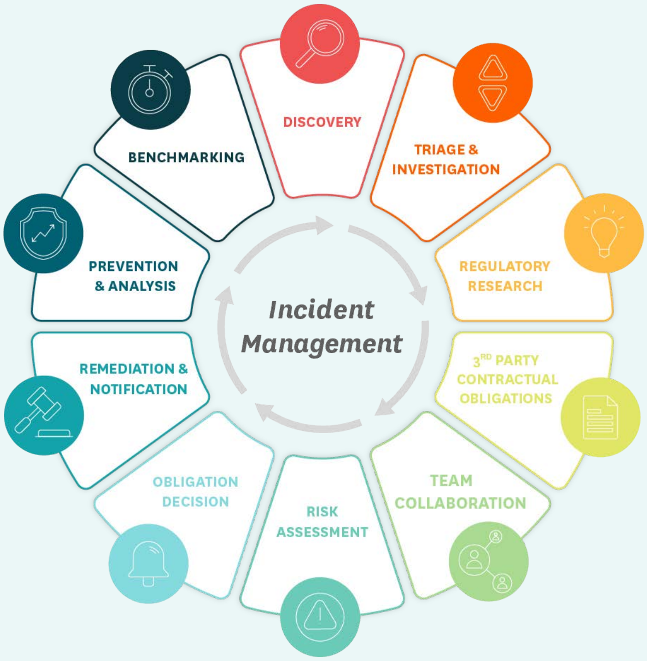
Identify Your Process in the Incident Management Cycle

Reporting does not happen in a vacuum. Often and simultaneously, teams must resolve events while managing incidents. Know that final resolutions can take anywhere from months to years.

In June 2023 a vulnerability was discovered in MOVEit, a managed file transfer software that immediately impacted thousands of organizations. Through November 2023 new breaches were discovered as a result of the event.

A Clear Process to Solve the Challenges of Incident Management while Reporting

Coordinating incident investigations requires a straightforward process to get the complete picture and reliable communications. Where the average data breach cost in the United States is 9.44M, you do not want to add to this cost with incomplete or poor-quality information.



RadarFirst's 10 Stages of Incident Management breaks down each stage of the Incident Management lifecycle.

Consider the first six stages — from "Discovery" to "Risk Assessment" — as information-gathering processes. You may also identify data gaps during these activities.

Then you will come to a Obligations Decision where you summarize what you learned and figure out whom to notify. At this point, your activities will turn to reporting.

Reporting Stages on the Incident Management Wheel

Three of the stages require reporting: Remediation & Notification, Prevention & Analysis, and Benchmarking. Before creating, updating, or producing a report, ensure your activities align with the stages below.

BENCHMARKING

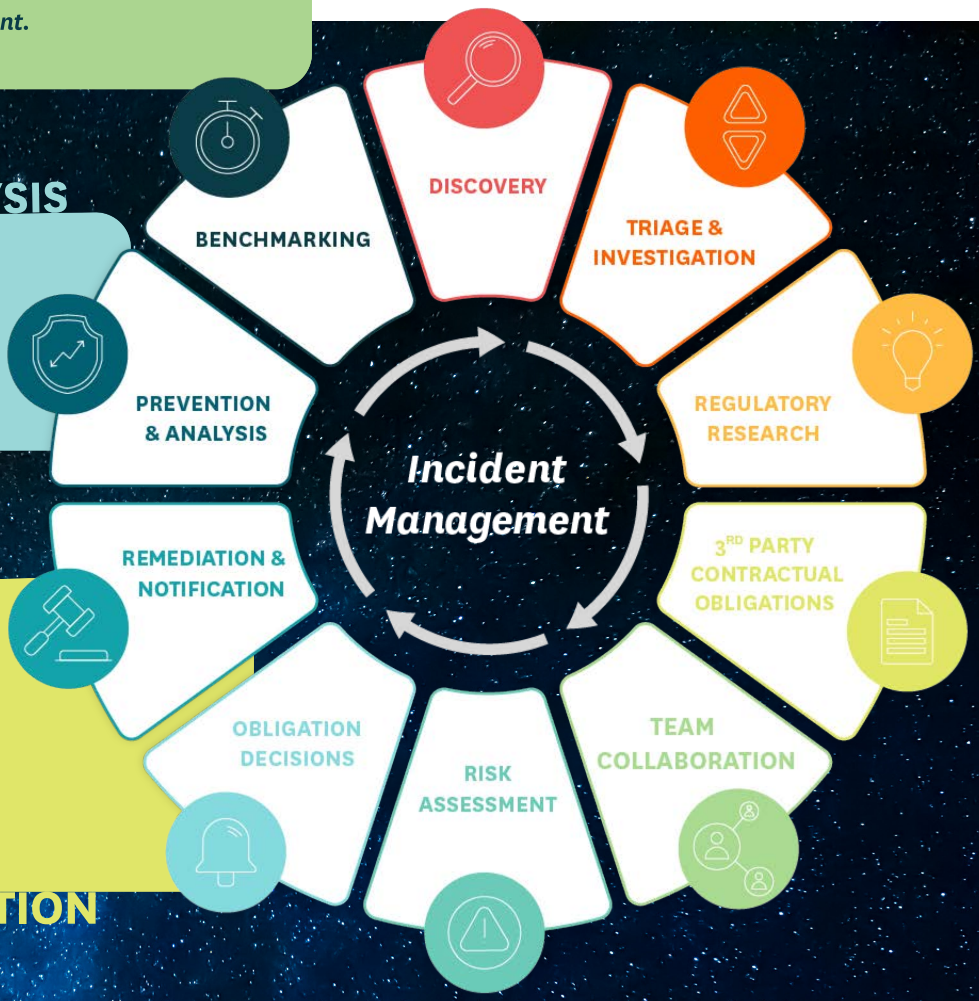
Benchmarking measures your company alongside other competitors and industry-wide trends to compare incident management and gain feedback for improvement.

PREVENTION & ANALYSIS

The incident team uses historical data to assess trends and understand root causes.

REMEDIATION & NOTIFICATION

A risk leader trains an audience around the organization about the incident, including through risk reporting.



A Maturity Framework for Risk Programs

Any organization faces a quickly changing regulatory landscape. In addition to increasing and quicker impacting data breaches, about 300 regulations require you to have incident management plans, and these laws all vary. Maturity measurements help organizations handle all these changes more effectively and efficiently by assessing adaptability.

Assessing Risk in Incident Management

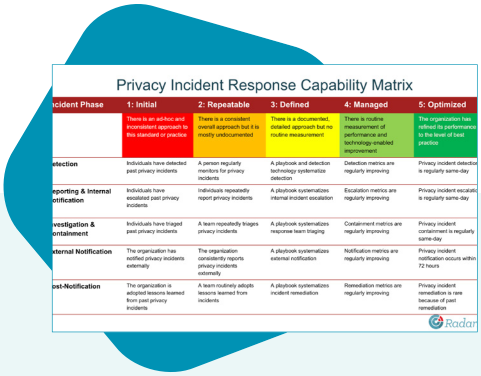
Upon categorizing an organization's incident management program, the evaluator must remember its general purpose to avoid getting fixated on a particular rating. So, objective evidence supporting an organization's maturity level drives resource identification for preparedness and how a risk program would best improve. Consider it a guestimate and a guidepost toward understanding business readiness in handling incidents.

ASSESS YOUR ORGANIZATION'S MATURITY LEVEL

In the previous section, this guide explained what activities required reporting and where they fit into the incident management picture. As you use the suggestions in the Maturity Framework for Risk Programs, remember that your rating will also reflect how well these report processes work.

ASSESSMENT TOOLS

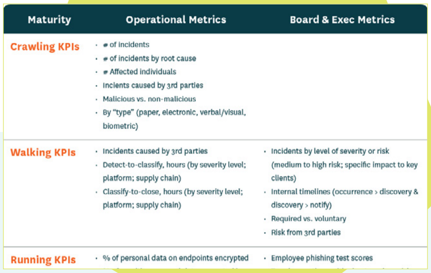
Due to the variety of privacy regulations with strict notification timelines, privacy incident response provides a great framework for risk reporting assessment. The following tools will help you rate your organization's maturity.



Privacy Incident Response Capability Matrix

cident Phase	1: Initial	2: Repeatable	3: Defined	4: Managed	5: Optimized
	There is an ad-hoc and inconsistent approach to this standard or practice	There is a consistent overall approach but it is mostly undocumented	There is a documented, detailed approach but no routine measurement	There is routine measurement of performance and technology-enabled improvement	The organization has refined its performance to the level of best practice
etection	Individuals have detected past privacy incidents	A person regularly monitors for privacy incidents	A playbook and detection technology systematize detection	Detection metrics are regularly improving	Privacy incident detectio is regularly same-day
eporting & Internal otification	Individuals have escalated past privacy incidents	Individuals repeatedly report privacy incidents	A playbook systematizes internal incident escalation	Escalation metrics are regularly improving	Privacy incident escalatic is regularly same-day
vestigation & ontainment	Individuals have triaged past privacy incidents	A team repeatedly triages privacy incidents	A playbook systematizes response team triaging	Containment metrics are regularly improving	Privacy incident containment is regularly same-day
xternal Notification	The organization has notified privacy incidents externally	The organization consistently reports privacy incidents externally	A playbook systematizes external notification	Notification metrics are regularly improving	Privacy incident notification occurs within 72 hours
ost-Notification	The organization is adopted lessons learned from past privacy incidents	A team routinely adopts lessons learned from incidents	A playbook systematizes incident remediation	Remediation metrics are regularly improving	Privacy incident remediation is rare because of past remediation

Radar



Maturity	Operational Metrics	Board & Exec Metrics
Crawling KPIs	· # of incidents · # of incidents by root cause · # Affected individuals · Inclents caused by 3rd parties · Malicious vs. non-malicious · By "type" (paper, electronic, verbal/visual, biometric)	
Walking KPIs	· Incidents caused by 3rd parties · Detect-to-classify, hours (by severity level; platform; supply chain) · Classify-to-close, hours (by severity level; platform; supply chain)	· Incidents by level of severity or risk (medium to high risk; specific impact to key clients) · Internal timelines (occurrence › discovery & discovery › notify) · Required vs. voluntary · Risk from 3rd parties
Running KPIs	· % of personal data on endpoints encrypted	· Employee phishing test scores

iapp

RadarFirst

The Privacy Incident Benchmark Report: Data to Drive Operational Excellence

Wednesday, March 25th, 2020

Time: 8:00–9:00 a.m. PT
11:00 a.m.–noon ET
5:00–6:00 p.m. CET

The Privacy Incident Response Capability Matrix

This model, provided by Jay Cline, serves as a great metric to measure improvement.

View Matrix »

KPIs by Audience, Drivers, and Maturity

Use this chart to demonstrate opportunities for improvement and funding or resources to kick off new training or testing.

View Chart »

Benchmarking: The International Association of Privacy Professionals (IAPP)

This slide deck helps you compare your privacy program to others through incident response data.

Open PDF in browser »

The Privacy Incident Response Capability Matrix

Incident Phase	1: Initial	2: Repeatable	3: Defined	4: Managed	5: Optimized
	There is an ad-hoc and inconsistent approach to this standard or practice	There is a consistent overall approach but it is mostly undocumented	There is a documented, detailed approach but no routine measurement	There is routine measurement of performance and technology-enabled improvement	The organization has refined its performance to the level of best practice
Detection	Individuals have detected past privacy incidents	A person regularly monitors for privacy incidents	A playbook and detection technology systematize detection	Detection metrics are regularly improving	Privacy incident detection is regularly same-day
Reporting & Internal Notification	Individuals have escalated past privacy incidents	Individuals repeatedly report privacy incidents	A playbook systematizes internal incident escalation	Escalation metrics are regularly improving	Privacy incident escalation is regularly same-day
Investigation & Containment	Individuals have triaged past privacy incidents	A team repeatedly triages privacy incidents	A playbook systematizes response team triaging	Containment metrics are regularly improving	Privacy incident containment is regularly same-day
External Notification	The organization has notified privacy incidents externally	The organization consistently reports privacy incidents externally	A playbook systematizes external notification	Notification metrics are regularly improving	Privacy incident notification occurs within 72 hours
Post-Notification	The organization is adopted lessons learned from past privacy incidents	A team routinely adopts lessons learned from incidents	A playbook systematizes incident remediation	Remediation metrics are regularly improving	Privacy incident remediation is rare because of past remediation

Provided by Jay Cline

KPIs by Audience, Drivers, and Maturity

Maturity	Operational Metrics	Board & Exec Metrics
BASIC **Crawling KPIs**	# of events # of events by root cause # Affected individuals Events caused by 3rd parties Malicious vs. non-malicious By "type" (paper, electronic, verbal/visual, biometric)	
INTERMEDIATE **Walking KPIs**	Events caused by 3rd parties Detect-to-classify, hours (by severity level; platform; supply chain) Classify-to-close, hours (by severity level; platform; supply chain)	Events by level of severity or risk (medium to high risk; specific impact to key clients) Internal timelines (occurrence > discovery & discovery > notify) Required vs. voluntary Risk from 3rd parties
ADVANCED **Running KPIs**	% of personal data on endpoints encrypted % of sensitive personal data encrypted in database columns Web application pen-test score Employee phishing test score Incident response maturity level Trends over time	Employee phishing test scores Trends over time, with plan to reduce risk Tabletop exercise results, tied to incident response maturity level

NOTES

2 Assess Your Organization's Maturity Level

In the Identify your Process in the Incident Management Cycle page, the guide explained what activities required reporting and where they fit into the larger risk management picture. As you use the suggestions in the maturity framework for risk programs, remember that your rating will also reflect how well these report processes work.

PUTTING TOGETHER THE ASSESSMENT

This maturity assessment helps evaluate its adaptability through its data-driven capabilities. A data-driven risk program ensures getting good metrics and understanding its context, the bedrock of any risk program.

ADVANCED

- Matches "Managed" or "Optimized" capabilities as shown in capability matrix
- Has Crawling, Walking, and Running KPIs as shown in the KPIs chart
- Has a coordinated and formalized event response across the organization
- Knows efforts to improve event response handling and their values
- Reveals above-average handling of risks during benchmarking

INTERMEDIATE

- Matches a "Defined" capability as shown in the capability matrix
- Has Crawling and Walking KPIs as demonstrated in the KPIs chart
- Has a coordinated and formalized risk management across the organization
- Reveals a risk program comparable to others during benchmarking
- Lacks knowledge about if or how the risk program handling incident management has improved.

BASIC

- Matches "Initial" or "Repeatable" capabilities, as shown in the capability matrix for one or more company divisions.
- Has Crawling KPIs only, as shown in the KPIs chart
- Lacks a formalized incident response across the organization
- Needs context around the metrics to make sense
- Reveals a significant gap in incident management during benchmarking

3 Identify Your Audience

Reports that make the most impact talk to the interests and needs of their audience. For this reason, you may need to highlight different content. Thanks to Judy Titera, MBA CIPP, Chief Privacy Officer at USAA, this guide has information on identifying these audiences and what they need.

Building a regular communication routine would be best regardless of who will see or hear your report. Your audience needs to trust you, and a sorry-for-data breach followed by immediate activity will not suffice. Instead, build a relationship with your audience and show quality and consistent performance to your promises.

Describing the Audience

Think of your readers or listeners as characterized by a set of characteristics:

UP

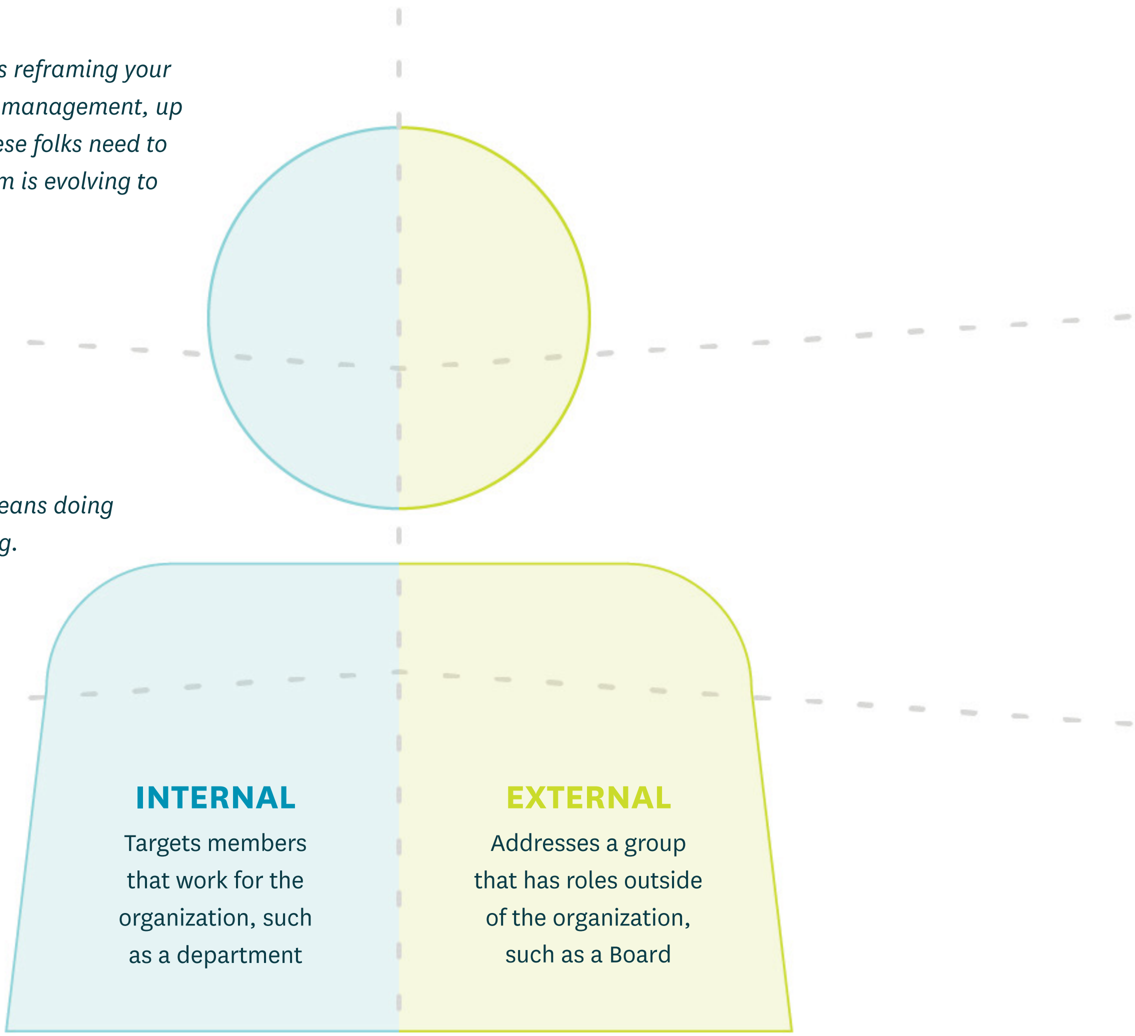
Communicating Up means reframing your risk report to higher-level management, up a pyramid to the CEO. These folks need to know how the risk program is evolving to serve their needs.

ACROSS

Communicating Across means doing organization-wide training.

OUT

People directly impact your risk program resource levels and financing, and your job is to inform them.



INTERNAL

Targets members that work for the organization, such as a department

EXTERNAL

Addresses a group that has roles outside of the organization, such as a Board

Some Audience Identities

Find examples below of specific groups you will report to. These audiences will expand as digital workloads, data breaches, and data value grow. So, feel free to add or modify the audience list as you see fit.

COMPLIANCE MANAGEMENT WANTS

- The trends in departments or organization units in how they protect data
- How notifications are handled, and to whom they go when there are risks
- An overview of specific stakeholder risk needs
- Enough information about any needed updates to policies or training
- The program's efficiencies in handling risk events

THE BOARD WANTS

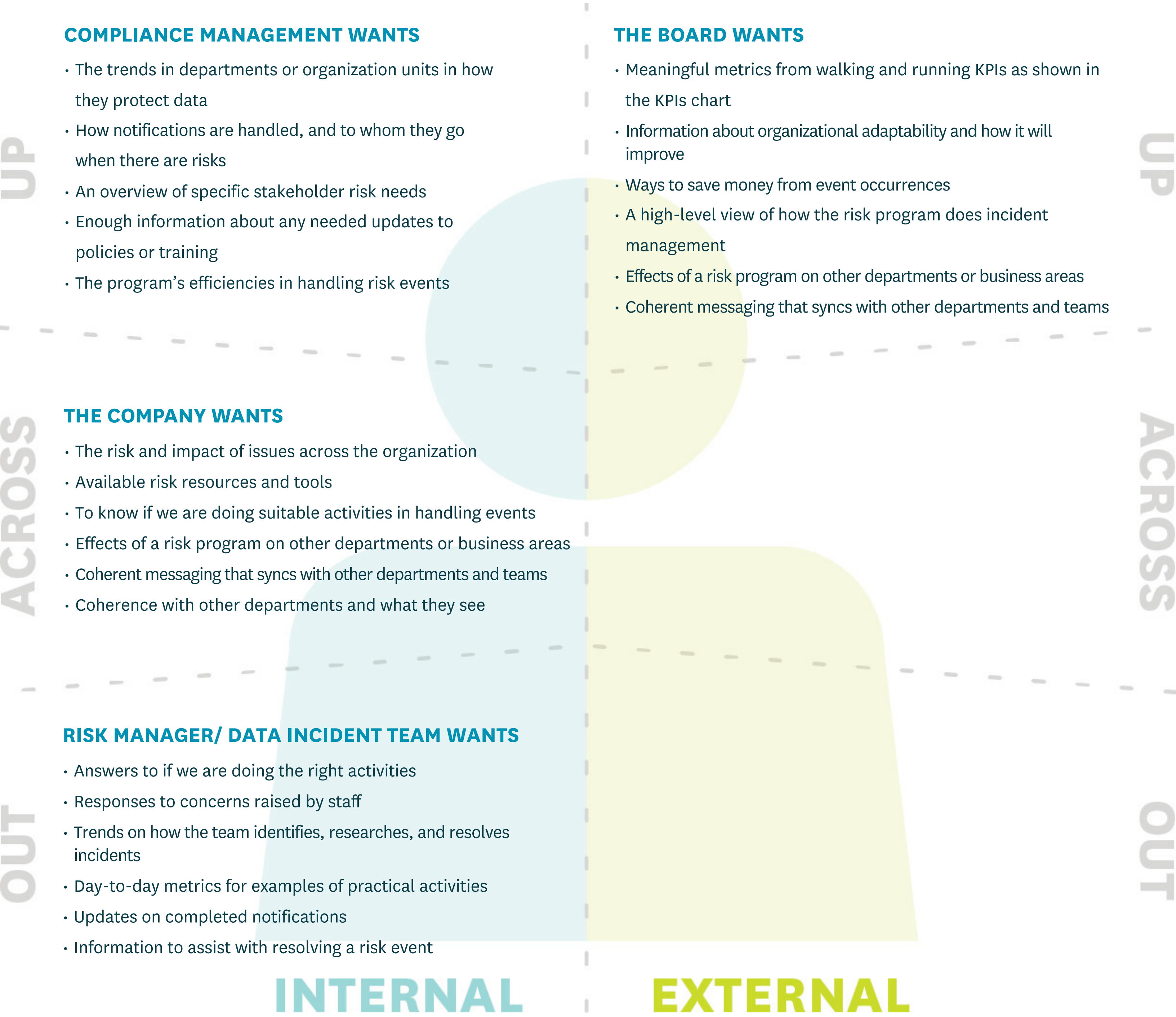
- Meaningful metrics from walking and running KPIs as shown in the KPIs chart
- Information about organizational adaptability and how it will improve
- Ways to save money from event occurrences
- A high-level view of how the risk program does incident management
- Effects of a risk program on other departments or business areas
- Coherent messaging that syncs with other departments and teams

THE COMPANY WANTS

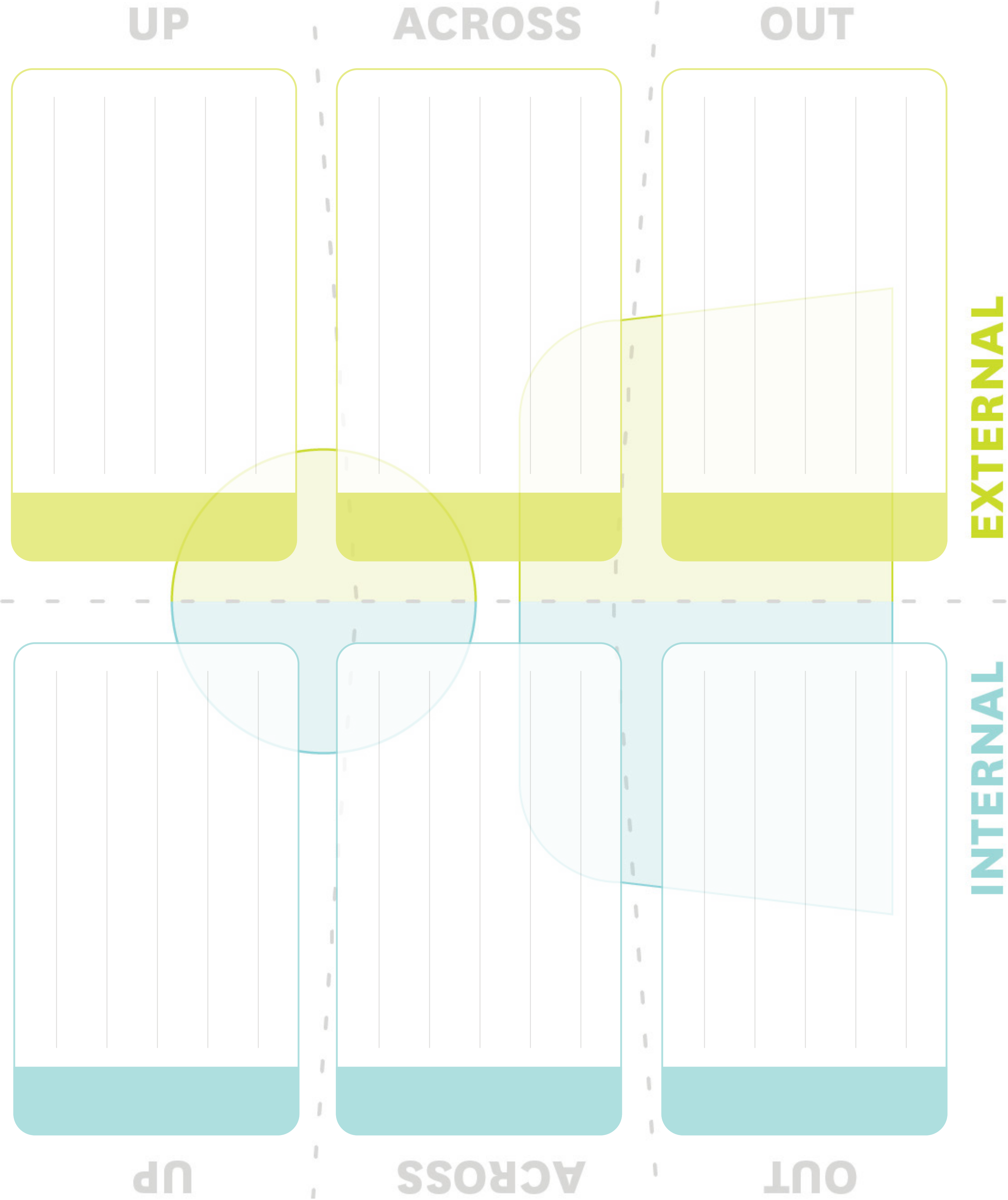
- The risk and impact of issues across the organization
- Available risk resources and tools
- To know if we are doing suitable activities in handling events
- Effects of a risk program on other departments or business areas
- Coherent messaging that syncs with other departments and teams
- Coherence with other departments and what they see

RISK MANAGER/ DATA INCIDENT TEAM WANTS

- Answers to if we are doing the right activities
- Responses to concerns raised by staff
- Trends on how the team identifies, researches, and resolves incidents
- Day-to-day metrics for examples of practical activities
- Updates on completed notifications
- Information to assist with resolving a risk event



3 Identify Your Audience | WORKSHEET



UP

ACROSS

OUT

EXTERNAL

INTERNAL

UP

ACROSS

OUT

4 Tell the Data Story

When you tell a good data story in your report, you leave your audience with a few impactful messages to take away and, perhaps, change their behavior. You also achieve your report's purpose.

To do so requires a good organization of your points and metrics to support them. This section will help you get an excellent structure to tell your data story by gathering information about the process steps in risk management, maturity, and the audience.

ORGANIZING THE DATA STORY

See the example below.

Audience: The Board

Stage	BASIC	INTERMEDIATE	ADVANCED
Remediation & Notification	• Briefly describe the event and those notified • Talk about organizational maturity and impact • Next steps including how to get to an intermediate level of maturity	• Follow your playbook/system for notification • Follow your playbook/system for remediation • Discuss how advanced maturity will lead to remediation and escalation improvements • Next steps backed up by crawling and walking metrics	• Briefly describe the event and those notified • Describe accomplishments in remediation and notification • Use crawling, walking, and running metrics to describe remediation and escalation improvement trends
Prevention & Analysis	• Summarize the event with available metrics • Describe the analysis gap and why using metrics about maturity • Discuss improvements to justify their ROI	• Explain the root cause of the event • Explain future risks and how they will be mitigated • Describe how advancing the organizational maturity will increase efficiency	• Explain the root cause of the event • Talk about the prevention trends that have reduced risk • Talk about improvement steps to prevent and analyze risks
Benchmarking KPIs	• Explain the benefits of benchmarking • Explain the processes and metrics behind those metrics • Discuss improvements to the risk program	• Show any benchmarking information • Explain about metrics needed to assess improvements • Show how risk management is on par and where it can improve	• Show benchmarking information • Celebrate where risk management is above average • Show how the program is improving and the next steps

4 Tell the Data Story | WORKSHEET

Audience: ______________________________

Stage	BASIC	INTERMEDIATE	ADVANCED
Remediation & Notification			
Prevention & Analysis			
Running KPIs			

Presenting the Data Story

Having strong content and organization helps a great deal, but you will need to format your report presentation for your audience.

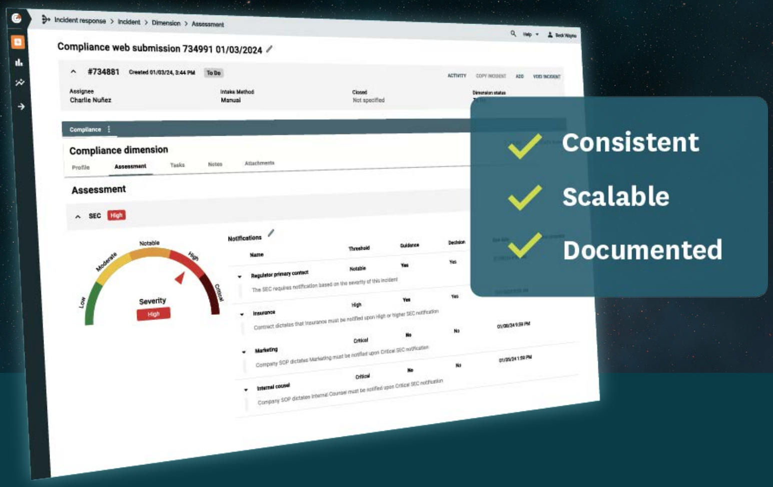
You will want to take stock of the business culture and present the information accordingly. For example, if a company emphasizes teamwork, praise teams who helped with risk management, and use language that suggests rather than dictates.

Go with an iterative approach in your risk reporting communications. Modify the content and presentation in future reports based on your audience's feedback.

SEE RADAR® COMPLIANCE IN ACTION

Find out why 99% of customers stick with RadarFirst

Schedule a Demo



Compliance web submission 734991 01/03/2024

#734881 Created 01/03/24, 3:44 PM To Do

Assignee: Charlie Nuñez
Intake Method: Manual
Closed: Not specified
Dimension status

Compliance dimension

Assessment

SEC High

Notifications

Name	Threshold	Guidance	Decision	
Regulator primary contact The SEC requires notification based on the severity of this incident	Notable	Yes	Yes	
Insurance Contract dictates that insurance must be notified upon High or higher SEC notification	High	Yes	Yes	
Marketing Company SOP dictates Marketing must be notified upon Critical SEC notification	Critical	No	No	01/30/24 9:59 PM
Internal cousel Company SOP dictates Internal Counsel must be notified upon Critical SEC notification	Critical	No	No	01/25/24 1:59 PM

RadarFirst

About RadarFirst

RadarFirst's award-winning governance, risk and compliance (GRC) software solutions are trusted by enterprises and organizations to reduce risk and simplify obligation decision-making. Radar® technology automates assessment processes to help companies meet time-bound response requirements and delivers transparent notification obligation decision-making against global data breach laws, as well as compliance and cyber regulations. With RadarFirst, organizations can define, streamline, and scale decision-making in a consistent, objective process.

TOP WORK PLACES
The Oregonian OREGONLIVE

Learn more at radarfirst.com.