LOGICGATE
CASE STUDY

horizonmedia

Overview

THE CUSTOMER
Horizon Media was growing fast. As a leading media services agency helping clients integrate their marketing strategy across traditional and digital media channels, their operations were expanding globally. They were storing increasing amounts of data in the cloud and needed to assure clients they could protect their assets and brands. Without a formal risk program in place, the company faced the monumental task of building one from scratch.

THE CHALLENGE
Establishing an effective risk program was an organizational challenge. Horizon needed to educate stakeholders on the value of a risk program, align their objectives and needs across the company, and build a shared culture of risk. To help, Horizon turned to LogicGate's Risk Cloud platform. The customizable and collaborative platform aligned with their people and processes while giving them the flexibility to grow with the company.

Today, Horizon benefits from a risk culture that protects their information assets and recognizes the value of a strong risk program. Read on to learn:

- How Horizon identified the objectives of their risk program and why those are different for each company
- Why focusing on what's important to the business can get you the resources to manage cyber and third-party risks
- How using the people, process, and tools methodology helps build a organization-wide culture of risk
- What an effective risk program looks like

Horizon Media:
Building a Risk Program from the Ground Up

Headquartered in New York City, Horizon Media is the largest and fastest-growing privately held media services agency in the world. Horizon had become an industry leader, in part, by using technology to gather business intelligence, measure channel connections, and employ data analytics.

With data and technology increasingly integral to Horizon's business, its risk infrastructure needed to evolve too. Horizon was operating in a highly virtual environment with a global client base, cloud-based operations, and multiple physical offices. With breaches and cyberattacks constantly in the headlines, Horizon needed a system to capture and monitor cyber risks (including those from third parties) and a cyber awareness training program to give clients the confidence that their data would be safeguarded.

Enter Praj Prayag, a technology risk executive with 18 years of IT audit, risk, and compliance experience at Big Four and top-tier financial services companies. Praj was hired by Horizon's CISO to build their technology risk program from the ground up. Recognizing the enormity of the task ahead of her, Praj knew that getting the resources and people she needed would require business support.

Before she came on board, risks were compiled in spreadsheets and not always considered when making strategic decisions. With risk operating independently from the rest of the firm, Praj knew she needed to educate stakeholders on the value of a risk program before she could build a shared culture of risk.

Setting Relevant Objectives

To design an effective technology risk program that met the firm's needs, Praj and her team needed to understand Horizon's broader objectives. Exploring why Horizon needed a technology risk program would help Praj socialize the idea and get the structure right.

Besides the standard objectives of protecting data and information assets and reducing organizational and cyber risk, conversations with business, technology, and executive leadership helped Praj understand that customer confidence hinged on strict levels of compliance. Clients needed assurance their data would be protected from unauthorized access, breaches, and cyberattacks. This would become a critical differentiator for Horizon's clients.

"Building a program that provides business value moves away from technology risk and audit being a cost center," says Praj "We enable businesses to grow by helping them achieve their objectives while keeping their data safe."

With that, Praj positioned the technology risk program as a key input to growth. Setting the program objectives in line with Horizon's business strategy smoothed the way for getting buy-in from business and resources for planning and implementation.

"Building a program that provides business value moves away from technology risk and audit being a cost center," says Praj. "We enable businesses to grow by helping them achieve their objectives while keeping their data safe."

Aligning People with Process

With support in hand, Praj used the people, process, and tools methodology to define what the technology risk program should look like and build efficiency and alignment across the organization.

The team agreed on four key pillars for their program: information risk management, third-party risk management, cybersecurity, and compliance and controls.

Praj and her team analyzed sources of risk in each area to understand the firm's critical risks and better prioritize their time and resources. Eventually, they defined discrete priorities and processes for each pillar.

Information Risk Management

Define an iterative, clear process that captures all the risk information and workflow

Third-Party Risk Management

Define a process to get vendor information and provide each vendor a risk questionnaire

Compliance and Controls

Create an annual plan for controls self assessment based on the annual risk assessment and compliance requirements

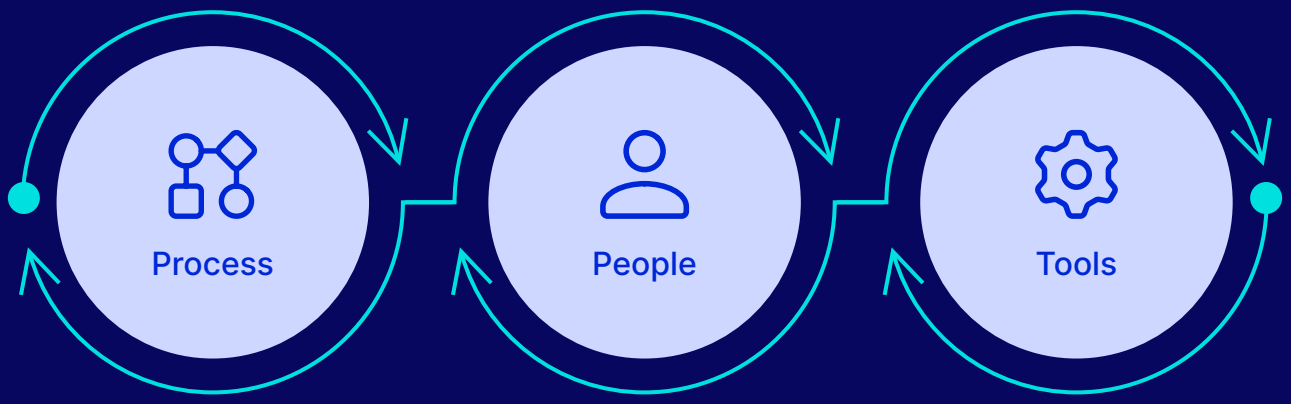
Cybersecurity

Centrally capture cyber risks and provide consistent cybersecurity training

Now that the vision and goals of their risk program were clear, they could move ahead with designing the appropriate structure.

Praj and her team recognized effective risk management was a firmwide responsibility. Identifying the right people to help with implementation was a key part of the process, people, and tools methodology. After designing the process for managing each pillar, they brainstormed about who they'd need to collaborate with and the resources required to manage those risks.

DEFINING THE TECHNOLOGY RISK PROGRAM



Process

- What are the key pillars of your Technology Risk program?
- How will the process for each of them work?
- Does the lack of one process have more significant business impact than the other?

People

- Who will be your partners for daily activities?
- Is technology and business on board with their time commitment?
- How many resources do you need to hire over each phase of the program? Will they be internal or external? Does that align with your budget?

Tools

- Does the organization have any existing tools that can work for this program?
- What tools will you need for automation and efficiency in each phase?
- What will the implementation for each of these look like?
- Will they have dependencies on other tools?
- What are your budget constraints?

Adopting the Right Tools for the Job

Once Praj and her team were clear on the risk management process and who they'd work with, they needed the right tool to serve their vision. It was important that the tool could align with how Horizon internally managed risk — they didn't want a tool that dictated to them how their process should work.

"Don't use the tool to drive your process. Define the risk life cycle process and identify roles and responsibilities, whether that's internal within the risk team or technology or the business before looking for a tool," Praj says.

INFORMATION RISK MANAGEMENT

1 Identify Risk

- Risk sources (vulnerabilities, incidents, audits, compliances, self reporting)
- Annual Risk Assessment
- Collecting information

2 Analyze Risk

- Impact v/s likelihood
- Scoring the risk
- Creating SLA's

3 Respond

- Risk remediation v/s acceptance
- Remediation plans and tracking
- Acceptance guidelines and approvals

4 Monitor and Control

- Track timelines
- Closeout risks
- Monitor risk acceptance
- Senior Management reporting & trends

Process

- Define an iterative, clear progress that captures all the risk information and workflow
- Set up SLAs and expectations

People

- Identify the teams that would provide bulk sources of the risks, and establish a methodology for the input
- Identify cross functional resources needed as per volume

Tools

- Identify the tool that would automate the process, create a central risk repository, and increase efficiency
- Ensure that all approvals are captured
- Provide training for the tool

Detailed diagrams of People, Process, and Tools for Cybersecurity & Awareness, Third Party Risk Management, and Compliance Readiness and Controls Self-Assessment can be found on pages 8 and 9, respectively.

LogicGate's Risk Cloud checked all the boxes. It was customizable to fit their needs, scalable with their risk program, and capable of evolving with their business. Praj and her team started small, beginning with the Risk Management Application, then expanding to the SOX Application for their compliance assessment, and later adding the Third-Party Risk Management Application. LogicGate now helps manage three out of the four pillars of Horizon's GRC Program.

Risk Cloud's flexibility and integrated reporting means Horizon can now:

- Collaborate and partner with business units to protect the firm's assets and reputation
- Align their compliance and risk management capabilities to business goals, whether that's PCI compliance or PII protection for their clients
- Improve cyber awareness across the organization through personalized phishing campaigns and preventative controls
- Proactively identify and address gaps in controls and compliance before they become a roadblock
- Systematically analyze and review vendors to minimize their third-party risk

"Cross-functional collaboration and management support can be a slow process, but building those relationships and talking in a language that business understands are keys to success."

"We have now lowered our threat landscape by more than 50% and are actively assessing every new technology vendor that we get into a relationship with, with the goal of monitoring the vendors, expanding to existing vendors and also expanding the risks that we manage," said Praj.

As Horizon's technology risk program matures, their goals continue to evolve with the business. Today, Horizon is looking for ways to infuse AI into their cybersecurity training and enhance overall process efficiency.

By aligning risk management processes with Horizon's strategic goals, Praj and her team have successfully built a culture of risk and proven their value to the business.

"If we focus on what is important to the business, and get the business onboard with reducing organizational risk as a whole, it can add tremendous value to the company," shared Praj.

CYBERSECURITY & AWARENESS

Process

- Provide Cybersecurity training
- Conduct simulated phishing campaigns and analyze data
- Define Policies and Procedures
- Implement preventative and monitoring controls
- Manage phishing incidents and communication
- Use Phishing campaign data to personalize training campaigns

People

- Collaborate with infrastructure and technology teams to build controls, monitor networks and manage incidents

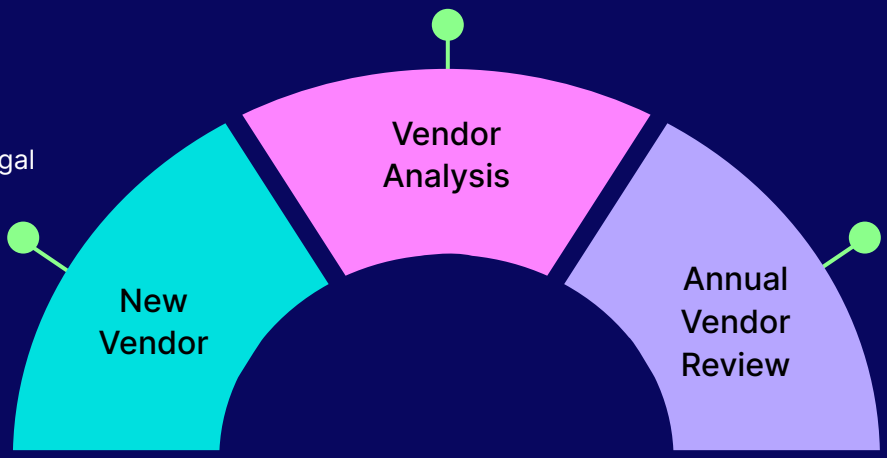
Tools

- Identify a Cybersecurity awareness tool that has strong content, scalability and maximum automation
- Advise technology teams on anti-phishing tools

THIRD PARTY RISK MANAGEMENT

- Analyze responses
- Review audit report
- Determine vendor risk

- Vendor intake form
- Collaborate with legal & procurement
- Provide risk assessment questionnaire



- Review changes with vendor
- Review existing and new vendor risks

Process

- Define a process to get vendor information and provide vendor a risk questionnaire
- Set up SLAs and expectations

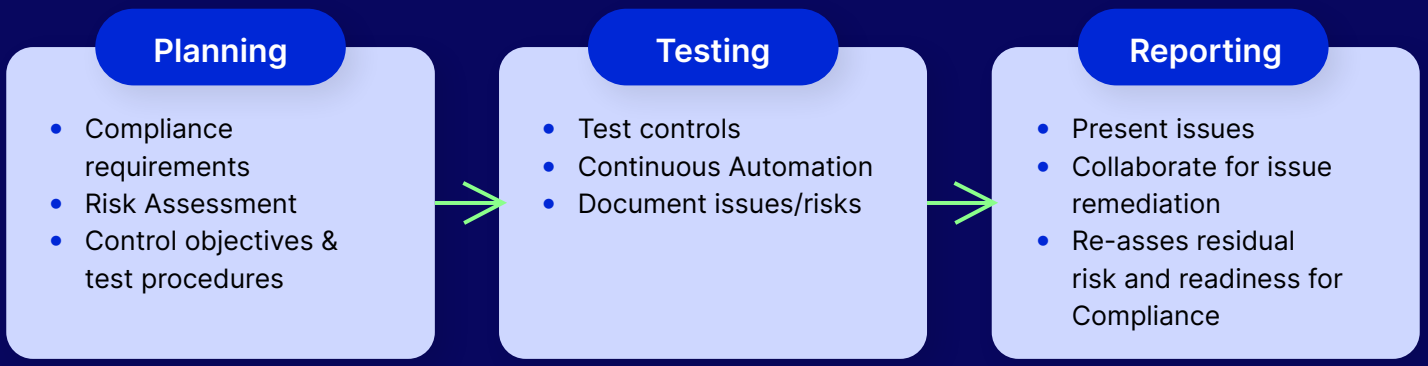
People

- Identify the roles and responsibilities for the risk team and the business teams
- Identify resources needed as per volume

Tools

- Identify the tool that would automate the process, create a central vendor repository, and increase efficiency
- Ensure that all approvals are captured
- Provide training for the tool

COMPLIANCE READINESS AND CONTROLS SELF-ASSESSMENT



Process

- Identify the compliance requirements
- Create a repository of control objectives
- Create an annual plan for reviews
- Perform readiness reviews and assessments based on annual plan and document risks
- Drive continuous automation initiatives in order to increase coverage of assessment

People

- Identify roles and responsibilities for the risk team and the technology teams, define timelines
- Collaborate with technology leadership for risk remediation

Tools

- Identify the tool that would automate the process, create a central risk repository, and increase efficiency
- Ensure that all workpapers, evidence and approvals are documented in the tool

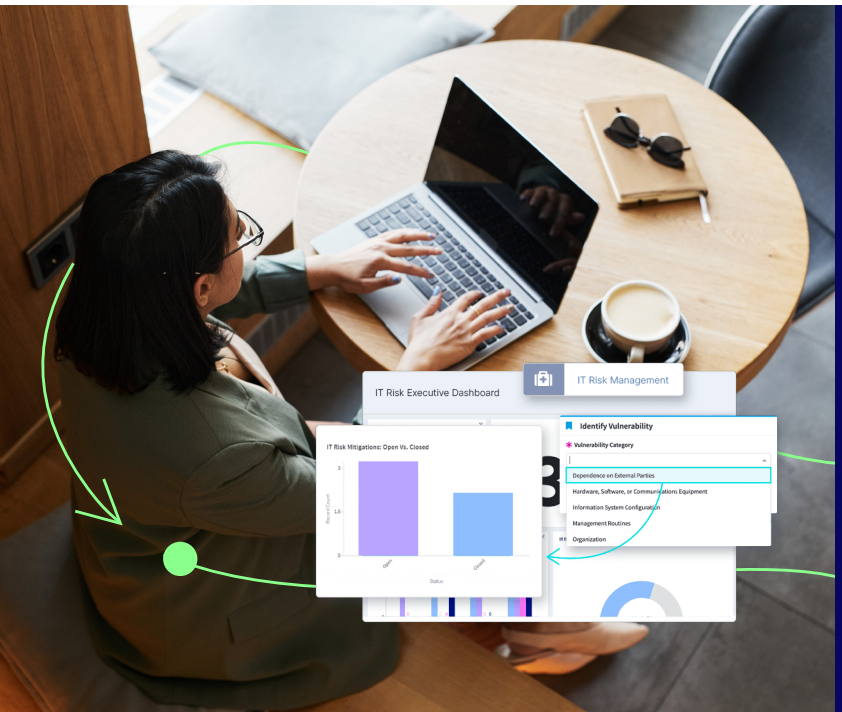
Since they were building the foundation of their technology risk program, they started with the basics — a tool that would identify, capture, analyze, and solve risk. But they wanted more than the essentials. The right solution needed to be:

- User-friendly to better collaborate across divisions and get users to adapt to the new process
- Have strong reporting capabilities for timely communication
- Efficient enough to be used by a small team without taking more time than a spreadsheet
- Centralized for an integrated view of the firm's cyber, compliance, and other risks
- Transparent for better tracking and accountability
- Scalable to grow with the firm

"You will never get every risk mitigated so use a more subjective and analytical approach. Helping business understand the impact or value of fixing a few critical risks or the cost of not addressing them will help you get business buy-in."

About Horizon Media

Horizon Media is the largest and fastest-growing privately held media services agency in the world. Through its mission "to create the most meaningful brand connections within the lives of people everywhere," the company has helped clients such as GEICO, Capital One, Corona, and LG develop their brand strategy and manage communications across traditional and emerging channels, including digital, social, and mobile.



About LogicGate

LogicGate gives you an interconnected view of risk across the organization that you just can't get from point solutions. After all, great companies are built not by avoiding risks — but by choosing the right ones.