Completely Covered

A Strategy Guide to Managing Company and Third-party Risk

Presented by

Thoropass™ | HITRUST®

Intro

As independent leaders in global compliance and risk management, Thoropass and HITRUST have championed frameworks, programs, and services that put companies' information and data security first.

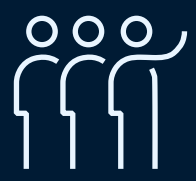
Thoropass, a compliance and audit solution working with customers since 2019, has revolutionized close-loop offerings in major compliance frameworks like SOC 2, ISO 27001, and HITRUST, where it is an external assessor. Through its customer-centric OrO Way, Thoropass provides compliance software and in-house audits with a particular emphasis on supporting risk-based cultures for growing businesses.

Since 2007, HITRUST has worked to empower organizations that are serious about security to elevate their cyber resilience and meet compliance requirements. HITRUST provides the one, universal framework and the assurance system that maps to all critical control sets, harmonizing over 50 authoritative sources. It provides the only assurance system that is adaptive to emerging threats for unmatched confidence. HITRUST offers a full portfolio of certification options that are streamlined and cost effective. And because organizations are only as secure as their least secure third-party vendors, HITRUST provides TPRM that is both powerful and pragmatic. When stakes are high, organizations count on HITRUST.

Together, Thoropass and HITRUST present a list of strategies and resources for managing company and third-party cyber risk.

In this guide

Chapter 01 Setting the foundation for third-party risk management



The concept of “risk” is ill-defined in many discussions about information security. Likewise, the related concept of “third-party risk management” (or TPRM) is also often loosely applied to any risk-related protocols of a business partnership.

However, the concepts are essential to get right — and in the right order — before a company can scale its business to meet security, compliance, and regulation goals. Thoropass and HITRUST have combined resources to demonstrate how companies can tackle this first step — moving from risk to third-party risk management — by creating a scalable strategy that puts infosec risk management and security at the foundation.

Laying the foundation for third-party risk management

Risk becomes the cornerstone on which everything else is built. As growing companies factor risk management into their business plans, it provides a lesson for even established companies to reassess their infosec plans both for the companies they are and the companies they want to be.

Before any business enters into a third-party agreement, it must have mechanisms to assess internal risk. Information security risk management involves identifying, evaluating, and mitigating risks associated with an organization's internal systems, processes, and data.

Understanding risk and establishing security controls

You can't protect what you don't know you have. And so, the first step in risk management is identifying and prioritizing your organization's critical assets and information.

Many of these risks will be fairly obvious depending on the company. For example, HealthTech companies will need to prioritize patient data in ways that FinTech companies will need to prioritize digital payments. But as a company goes deeper, it must look at the multiple inputs and outputs of its assets.

Once internal risks are assessed and categorized, organizations need to establish adequate internal security controls. These controls include policies, procedures,

technical safeguards, and employee training.

For example, creating a risk matrix (typically a 4×4 grid, sometimes called a risk register) based on controls and monitors specific to the company can be a helpful first step for companies making the motion from looking inward to outward. Having a robust internal security posture enhances the ability to demand and enforce security measures from third parties.

Assessing risk appetite and building trust

The threat of risk, unfortunately, never entirely goes away. Companies, compliance frameworks, and regulations do their best to minimize an organization's exposure to risk. Still, with new technologies and threat actors constantly emerging, companies must ultimately assess what they're willing to expose themselves to and by how much. Essentially, they must weigh the risk of risk.

Understanding a company's risk appetite is a critical component of risk management. It guides decisions on

what risks are acceptable and what controls are necessary. It also provides a baseline for evaluating third-party risks against the organization's risk tolerance.

When organizations can demonstrate their commitment to information security, it instills confidence in third parties and makes collaboration smoother. It likewise meets the base requirements that are precursors to a broader TPRM strategy.

Moving from risk to third-party risk management

A business cannot pursue effective TPRM without first putting in the time to establish proper risk management. By addressing internal risks first, organizations can create a secure foundation and extend their risk management efforts to external relationships more confidently.

Beyond internal assessments, the first big step is exploring compliance with relevant laws and regulations. Some of this entails fundamental legal issues. But as patient data rights are concerned, covering your risk via a self-reported HIPAA certificate to a HITRUST CSF framework is a significant step forward.

As we continue through this guide, keep this potential linear path of risk to TPRM in mind: though there is no single path to TPRM, there also aren't any easy shortcuts.

Chapter 02 What is risk management in compliance?

Infosec compliance risk management involves identifying, evaluating, and mitigating potential losses stemming from the failure to adhere to laws, regulations, and standards, as well as internal and external policies and procedures.

By keeping up with the latest rules and regulations, organizations can minimize non-compliance risks to avoid legal penalties, financial losses, and reputational damages.

3 key components of compliance risk management

To effectively manage compliance risks, organizations must have a robust compliance risk management program, including the following:

1 Policies and procedures

By having well-defined policies and processes, organizations can ensure they address all compliance requirements. Examples of compliance policies and procedures include:

- Data security policies
- Incident response plans
- Employee training programs

In addition, compliance contracts can help ensure adherence to terms and conditions, thereby minimizing the risk of fraud, corruption, and reputational damage.

2 Risk assessment

The risk assessment process involves examining various factors, such as the organization's operations, industry, size, and geographical location, to determine the likelihood and impact of non-compliance.

Organizations can use the results to develop an enterprise risk management strategy focusing on compliance risk.

3 Monitoring and reporting

Sometimes, it can be challenging to see something you're not tracking. Ongoing monitoring and reporting of compliance efforts are vital for maintaining transparency, accountability, and continuous improvement.

By regularly reviewing and updating policies, procedures, and training programs, organizations can create a culture of compliance that not only meets regulatory requirements but also promotes ethical behavior and accountability throughout the organization. In essence, compliance is a collective responsibility, not just an individual's duty.

Chapter 03 How to unlock the power of risk management

Risk is a combination of business, governance, regulatory, and security/privacy factors that organizations must manage to ensure compliance.

To manage risks effectively, organizations should adopt best practices to identify and address potential risks, allocate resources efficiently, and maintain industry regulatory compliance.

Periodic and continuous risk assessment

Regular and consistent risk assessments are crucial for identifying and addressing potential compliance risks. According to the NIST RMF (Risk Management Framework), there are seven steps involved in conducting a risk assessment:

1. Prepare: Prepare the organization to manage security and privacy risks.
2. Categorize: Categorize the system and information processed, stored, and transmitted based on an impact analysis.
3. Select: Select the set of controls to protect the system based on risk assessment(s).
4. Implement: Implement the controls and document how controls are deployed.
5. Assess: Determine if the controls are in place, operating as intended, and producing the desired results.
6. Authorize: Make a risk-based decision to authorize the system.
7. Monitor: Continuously monitor control implementation and risks to the system.

Risk ownership

Assigning risk ownership is essential for accountability and effective risk management. Designating a risk owner ensures each risk is managed by the appropriate team or individual responsible for identifying, assessing, and

mitigating the risk within the project or organization.

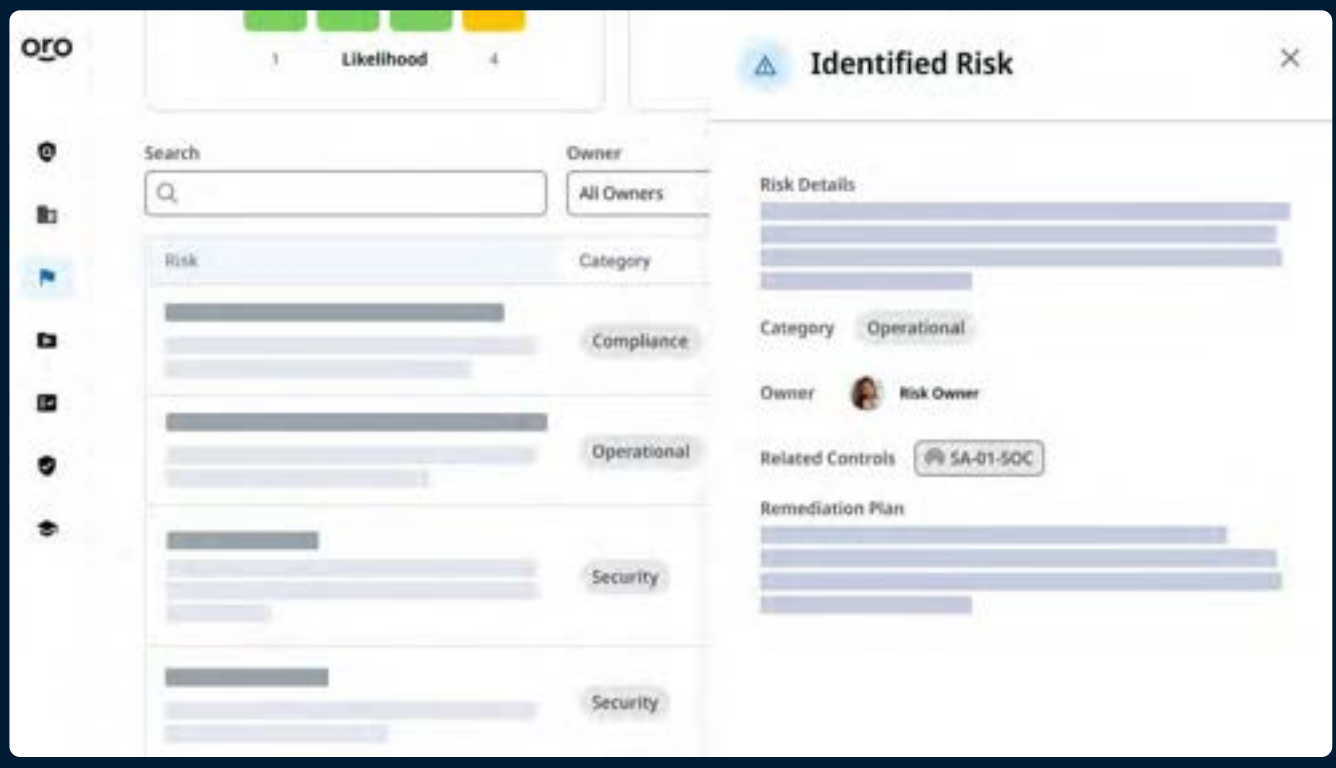
Assign risk owners based on factors such as:

- Accountability by position
- Ownership based on location
- Ability to manage risks
- Clear articulation of risks

Components of a risk register

A risk register (a 4×4 or 5×5 grid discussed in Chapter 1) is a powerful risk management tool that enables organizations to identify, categorize, and prioritize potential risks. It includes components such as:

- Risk identification and cataloging
- Risk analysis and assessment
- Mitigation strategies



Identifying potential risks

Identifying potential risks is the first step in constructing a risk register, which involves gathering input from team members and stakeholders, considering industry-specific risks, and using historical data to inform risk identification.

Documenting and monitoring risks

Documenting risks in a risk register is essential for tracking progress, implementing mitigation strategies, and communicating risks to stakeholders. Documenting risks involves recording the risk identification, description, probability, impact, response plans, and risk owner in the risk register.

Regularly reviewing and re-evaluating risk information helps organizations determine any changes and assess the status of risks.

Keeping up with emerging risks

As new risks emerge, organizations must adapt their risk management strategies to address challenges and maintain compliance. Some techniques include horizon scanning, adopting a formal risk assessment process, and improving the risk management framework. Implementing these strategies keeps organizations proactive and prepared in managing developing risks, ensuring effective responses to new challenges, and maintaining compliance with industry regulations.

Chapter 04 The importance of TPRM

Companies, large or small, work with many third parties for their business operations. You may have a vendor who manages your payments and invoices, a supplier who provides essential equipment and devices, and a cloud service provider (CSP) to store your data on the cloud.

Your organization relies on vendors, producers, or partners. Whenever organizations share data and vulnerabilities, they are engaged in a third-party business relationship that warrants risk management.

More third parties, more risks

Organizations rely on third-party vendors for crucial functions. However, as these vendors work more closely with your systems, the vendors often gain internal access to sensitive data. As dependencies increase, the risk of cyber threats increases, too. You may have a robust cybersecurity program. But what about your vendors? How do you ensure they have a strong cybersecurity plan to protect your and your customers' data?

The answer to these questions sets the foundation for how an organization establishes and maintains its TPRM program.

TPRM in compliance

Whether a company is looking to be an assessor or assessed, compliance is essential in setting ground rules for how risk is addressed in any business partnership.

Integrating TPRM into your compliance programs allows you to extend risk management efforts beyond the confines of your organization's internal infrastructure. By proactively assessing and mitigating the risks associated with external vendor relationships, for instance by using Thoropass's Due Diligence Questionnaire (DDQ) feature, you can safeguard your organization's data assets, protect against potential vulnerabilities, and ensure compliance with regulatory mandates.

One of the key reasons why TPRM is indispensable in building a compliance program is the inherent interconnectedness of today's business ecosystem. Any weaknesses or breaches within a third-party vendor's infrastructure can have cascading effects on your organization, making it imperative to assess and manage these risks effectively. Your company is as strong as its weakest third-party partner.

Regulatory reasons for TPRM

Regulatory bodies are placing greater emphasis on holding organizations accountable for their third-party vendors' security and privacy practices. Compliance requirements such as GDPR, HIPAA, and CCPA extend not only to internal data handling but also to the processing and storage of data by third-party entities. Failure to ensure third-party vendors' compliance can result in severe penalties, legal ramifications, and damage to your organization's reputation.

Incorporating TPRM into compliance programs enables you to demonstrate due diligence and regulatory compliance to stakeholders, auditors, and regulatory authorities.

Chapter 05 Why the old TPRM is broken

Organizations struggle to protect their data from attackers, and data breaches have become a common problem. According to Verizon's 2023 Data Breach Investigations Report, attackers access an organization's data by stealing passwords, phishing, and exploiting vulnerabilities. Perhaps not surprisingly, 74% of all breaches involve the human element, including error, misuse, and social engineering.

Third-party partners can be used as an access point to an organization's sensitive data. Effective TPRM is critical to ensuring your third-party vendors appropriately safeguard your data.

But all vendors are not the same. They differ in size, scope of work, risk profile, and cyber maturity. As you deal with varying volumes of diverse third parties, vendor risk management becomes challenging.

Existing TPRM solutions are incomplete:

- Most approaches to TPRM lack a consistent, widely available risk reporting approach.
- TPRM teams have limited bandwidth and resources.
- TPRM teams can't keep up with the high volume of vendor assessments.
- Vendors are overwhelmed with repetitive proprietary questionnaires and audits.

Over-reliance on outdated systems

Some organizations lack any form of risk or TPRM awareness. However, even those that do often rely in part or overall on outdated, incomplete, and manual methods to handle the many tasks that go into having a successful system.

Outdated approaches to TPRM involve cumbersome processes such as spreadsheets, email communications, and disparate tools, making maintaining an accurate and comprehensive view of third-party risks challenging. These methods are inherently limited in scalability and prone to human error, leading to gaps in risk assessment and delayed response times.

Moreover, manual TPRM lacks the agility to adapt to the rapidly evolving threat landscape and regulatory environment.

TPRM that doesn't work for the company

Incomplete TPRM processes often result in siloed data and fragmented insights, making it challenging to gain a holistic understanding of third-party risk exposure across the organization. CISOs and risk teams are tasked with piecing together disparate information from various sources, hindering their ability to make informed risk management decisions.

Many companies begin with modest TPRM goals, but even if they can meet them initially, they often can't keep pace with the growing number of third-party relationships. As businesses expand their ecosystems, managing third-party risk becomes increasingly complex and resource-intensive. Manual processes simply cannot keep pace with the scale and velocity of modern business operations, leading to inefficiencies, compliance gaps, and increased exposure to cyber threats.

Chapter 06 Best practices to enhance TPRM

Despite inherent problems with how many organizations address TPRM, there are clear and straightforward ways for a company to establish a sustainable and effective TPRM approach.

Use clear language in contracts

Ensure your contract language is clear and concise. The contract should specify the scope of the system and data. It should support risk assessment and ensure all stakeholders have common assurance expectations. Further, the contract should mention data ownership, use, and management requirements, along with risk management and security expectations.

Assess third parties based on their risk levels

Some vendors are at a higher risk than others. It is important to have a risk-tiering strategy to meet appropriate security requirements. Consistent risk analysis allows you to assess high-risk vendors without ignoring low-risk ones. When performing risk analysis, ask the following questions to determine the correct level of security assurance needed for each third-party partner:

- What data does the vendor process?
- If the data is compromised, how will it impact your organization?
- How important is that third-party vendor for your business?
- What are your responsibilities toward security and compliance?

Choose a reliable assurance mechanism

Choose a trusted, reliable assurance mechanism to ensure the third party takes proper security measures. Check if the assurance mechanism is transparent. You should know

the source of the controls. The control system should be well-recognized. Next, ensure that the assurance mechanism is consistent.

Assessment results should be the same irrespective of the assessor. The specified controls should be comparable to another organization's assurance report.

Go with an accurate assurance mechanism. It should use a detailed and quantitative scoring methodology. Finally, check that the assurance mechanism maintains integrity. Ensure the assessors are trained and conducting assessments faithfully.

Parameters of a reliable assurance mechanism are: Transparency, Consistency, Accuracy, and Integrity.

Review CAPs to track progress

The assurance report suggests gaps in the security system. The next step for third parties is to create Corrective Action Plans (CAPs) to rectify control implementation. You must work with your third parties to ensure they take suitable measures to meet the gaps. Check if the timelines are set correctly and track their progress.

Update assurance regularly

Security requirements are flexible and change constantly. New threats emerge with time. As the business grows, the potential risk level may increase, too.

Third parties should update their assurance regularly.

Updated assurance reports ensure relevancy and prepare the vendors against emerging threats.

Use a systematic approach to manage multiple third parties

Your organization works with numerous third-party vendors and suppliers belonging to different industries. These vendors and suppliers work with other third parties. Due to the many stakeholders involved, a technological, systematic approach is necessary for efficiency.

Use a system that checks progress across multiple stakeholders, supports results sharing, and aligns with existing systems and relationships. Ensure that it allows you to narrow the analysis based on specific needs. Moreover, pick a system that facilitates effective communication among all parties.

Chapter 07 How to build a risk-based culture

Having seen times when risk assessment programs have failed and those times when they have flourished, it is clear that certain key attributes are critical to building a solid risk management program, one that ultimately builds and enhances business value.

Guiding a business requires alignment from top to bottom. At the top, it starts with the board. Public boards are increasingly being held accountable for cyber risk, so much so that they are being asked to ensure that they have expertise on their board of directors. These positions will go to people who will ask the right questions and ensure that a company's risks are properly managed and prioritized.

From the boardroom to the cubicle, companies that foreground risk are seen as the surest bet for investment and trust.

4 steps to building a business through risk management

1 Build an open and transparent culture that supports risk awareness

- Companies that are transparent and share information with stakeholders regularly about matters affecting the business are best suited to having a strong risk culture. This helps ensure that every employee at every level feels like a co-owner and collaborator for the business's future direction.

- An open and transparent culture encourages people to have open dialogue, share concerns, and ultimately raise red flags when required.

- This doesn't mean every risk is critical and must be prioritized and mitigated. But it does mean that raised issues are documented and the right people are debating the issues' validity, including the likelihood of a risk occurring based on data and facts and, ultimately, the impact of the risk.

2 Establish strong governance and accountability

- Identify a clear, independent owner for a governance process and someone who has credibility with their peers and business partners.

- This means they deeply understand the business, the technology, and the potential financial, reputational, and regulatory risks.

- This individual should have access to data and information to support the risk process that starts with risk identification.

- Measures should be taken to quantify the impact of risks properly. This should be customized and unique because, for example, a payment platform that handles and stores credit card data has different risks than a chat application that hospitals use to share personal health information with patients.

- Tracking risk levels over time is critical. The material should be documented and shared every quarter.

- Finally, the company must make a regular review of historical decisions. Planning for the future always starts with examining the past.

3 Invest in tools and measure

- Having the correct data, monitoring trends, setting expectations, and creating visibility are critical to making the most informed business decisions. Invest in tools to help track risks across the company.

- Establish Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs), and monitor trends that signal there may be changes in the risk profile of a business or functional area.

4 Tie responsibility to compensation

- Any performance-based culture that factors in risk management for every business head will more likely avoid the perils experienced by SolarWinds. P&L performance, Risk, and Customer Satisfaction are three core tenets important to a balanced scorecard approach for executive compensation.

- Finally, if a failure causes financial or reputational damage, compensation for accountable executives (and others) should be impacted. Especially in situations where escalations have been repeatedly deprioritized, executives need to be held responsible for the business/risk decisions they make (or don't make), and the organization needs to demonstrate that they take these responsibilities seriously.

Together, these four steps can lead to better business decisions by properly prioritizing risk management as part of a larger strategy.

Chapter 08 How to attain efficient TPRM

Constructing a reliable internal risk program and scalable TPRM program is essential to any business. In addition to the tips provided in the previous chapters, any organization looking to build a TPRM program should follow these steps:

1 Define Objectives and Scope:

Begin by clearly defining the objectives of the TPRM program and its alignment with compliance requirements. Identify key stakeholders, including legal, procurement, and business units, to ensure comprehensive coverage of third-party relationships.

2 Conduct Risk Assessment:

Perform a thorough risk assessment to identify and prioritize third-party risks based on factors such as the criticality of services, data sensitivity, and regulatory requirements. Thoropass's Risk Register is one way to do this.

3 Implement Due Diligence Measures:

Develop a structured due diligence process for evaluating and onboarding new vendors, incorporating security requirements and compliance obligations into contractual agreements. Establish criteria for vendor selection based on security posture and regulatory compliance. Thoropass's DDQ tool is one way to do this.

4 Establish a Governance Framework:

Develop a governance framework to oversee the TPRM program. Form a cross-functional TPRM committee comprising legal, compliance, procurement, and IT security representatives to provide oversight and guidance. HITRUST CSF is one way to do this.

5 Continuous Monitoring and Improvement:

Implement continuous monitoring mechanisms to track changes in vendor risk profiles, security posture, and

regulatory landscape. Stay abreast of emerging threats and vulnerabilities impacting third-party relationships and adapt TPRM strategies accordingly.

The simplest way to implement these best practices is by utilizing Thoropass's compliance-based approach to risk and establishing a compliance-forward program such as that offered by HITRUST.

- Thoropass offers a Risk Register tool that can help companies identify risks.
- Thoropass offers a Due Diligence Questionnaire (DDQ) that can be used by companies or requested of their third parties. HITRUST offers reliable assurances that are based on the HITRUST CSF.
- The HITRUST CSF is accepted widely.
- You can access the CSF easily to determine the sources of the controls.
- The CSF is mapped to multiple authoritative sources, ensuring consistency.
- The HITRUST scoring methodology is based on a quantitative model, making the results unbiased and accurate.
- HITRUST trains assessors (including Thoropass) to follow a standard process, ensuring integrity.

HITRUST offers three certification options based on vendor needs, size, risk maturity, and business profile.

The HITRUST Essentials (e1) Validated Assessment is ideal for low-risk vendors seeking to establish foundational cybersecurity or more complex organizations looking to start their certification journey with plans to move into a more comprehensive certification level.

The HITRUST Implemented (i1) Validated Assessment offers more coverage than the e1. It is suited for third-party vendors demonstrating leading security practices.

The HITRUST Risk-Based (r2) Validated Assessment is its most comprehensive assurance. It is considered the gold standard in the industry and is ideal for high-risk vendors.

Each level is built on a common framework. This means your third-party partner can begin with a lower-level assessment and move up to a higher level without losing the invested time, money, and effort.

HITRUST Results Distribution System (RDS)

The HITRUST Results Distribution System (RDS) offers a secure electronic portal to share results. It helps you save time and effort when managing multiple third parties. You no longer need to locate assessment results and enter data into your TPRM solution manually. The RDS enables better compliance and analytics.

It can upload assessment details into TPRM solutions instantly and efficiently. It streamlines receiving and analyzing assessment results.

Conclusion

The success and growth of businesses hinge upon the ability to manage both internal and external risks effectively. As stewards of cybersecurity, you and your team must recognize the critical importance of maintaining successful internal risk management programs alongside robust TPRM initiatives.

Internally, a successful risk management program ensures the protection of sensitive data, critical assets, and intellectual property from internal threats such as insider breaches, human error, and system vulnerabilities.

Externally, third-party relationships introduce a myriad of risks that can impact business continuity, compliance, and reputation. Without a comprehensive TPRM program in place, organizations are vulnerable to security breaches, data leaks, and regulatory penalties stemming from the actions or vulnerabilities of external vendors, partners, and service providers.

Thoropass and HITRUST represent two stops on the compliance continuum that lead to a company's successful security posture. The synergy between internal risk management and third-party risk management is essential for the sustainable growth and resilience of businesses. By prioritizing both aspects of risk management, CISOs can effectively navigate the complexities of modern business operations, mitigate threats, and capitalize on opportunities for innovation and expansion.

For more information visit:

Thoropass™

thoropass.com

HITRUST®

hitrustalliance.net