Building a Third-Party Risk Management Program from the Ground Up

What Every CISO Needs to Know

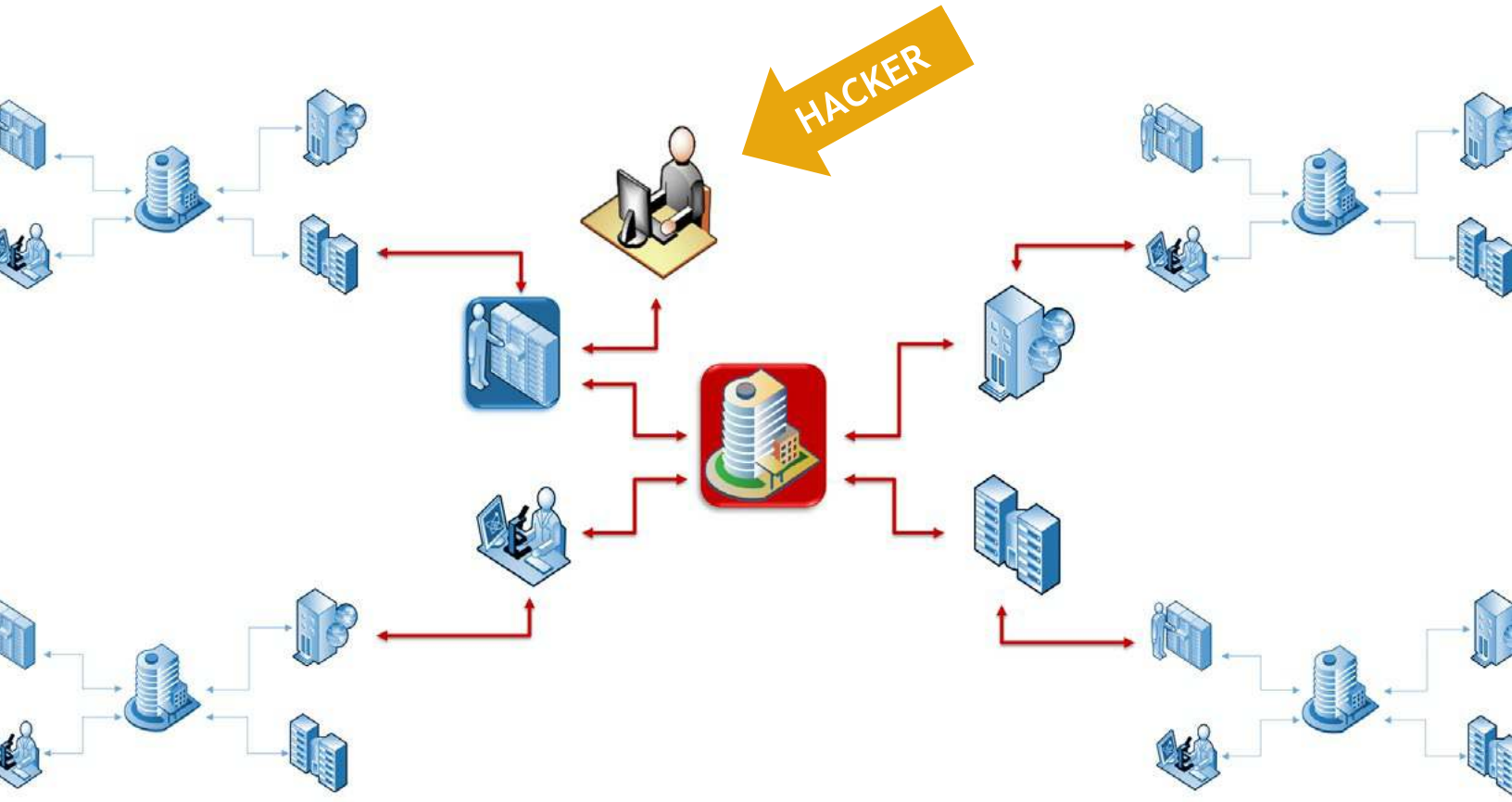
Intraprise HEALTH

Secure with Vigilance. Engage with Insight.

Table of Contents

Introduction: Third-party data breaches — how prepared are you?

As a CISO, CIO or board member of a healthcare organization, you know how important it is to safeguard protected health information (PHI) and personally identifiable information (PII). As a seasoned tech-enabled healthcare information security firm, Intraprise Health has extensive experience creating strong cybersecurity programs for healthcare organizations and believes there are a number of best practices all CISOs should follow in building a mature security program for their own organization.



A primary component of a comprehensive security program is third-party risk management, or TPRM, which helps you manage risks posed by third parties your organization has hired to provide software and/or services. Many of these vendors have access to your data and may jeopardize the security of your organization's information because they don't have strong security practices themselves. Simply put, it is your responsibility to ensure that your healthcare organization is assessing and minimizing the risk when anyone other than you touches your data.

Defining the problem: The facts, just the facts

Since 2009 there has been a steady increase in year-over-year healthcare data breaches, which have totaled over 3,000 breaches involving 500 or more records. Those breaches have resulted in the disclosure of over 231 million healthcare records, equivalent to almost 70% of the American population.

According to the Office of Civil Rights, halfway through 2019, more healthcare records were breached than in all of 2016, 2017 and 2018 combined. More than 35 million individuals had their healthcare records compromised, exposed or impermissibly disclosed last year.

In a Ponemon Institute survey of 600 Chief Information Security Officers (CISOs) and other information security professionals on what they worried about most, 42% of respondents reported a third-party data breach was highest on their list. Additionally, 60% of respondents said their concern about experiencing a data breach caused by a business partner, vendor or contractor (third party) increased (39%) or increased significantly (21%) over the previous year.

When asked why they think they will have a data breach or attack, the majority of respondents, 65%, said they had inadequate in-house expertise. Failure to control third parties' use of our sensitive data netted a 51% response. Each breached health record costs organizations more than $400 per record in the form of restitution, reparations, legal fees and reputation, adding significant cost burdens to the affected entities. Many companies have filed for bankruptcy due to a breach.

While third-party risk management is a relatively new concept, it's now on the mind of nearly all executives. The costs associated with third-party breaches make a strong case and represent a large financial stake for covered entities to make sure their bases are covered.

And while HIPAA regulations require a written promise to properly handle data, some business associates (BAs)/vendors may believe they have a strong security program when in fact, they are exposing your organization to great risk. Most organizations use many different vendors to provide products and services — exposing your organization to not only third-party breaches but fourth-party and beyond. When these BAs are hacked, they can serve as a conduit through your organization's security perimeter. The impact can proliferate throughout the organization.

The number of healthcare data breaches in the US annually has increased 30x over the last 11 years, from 18 in 2009 to 510 in 2019. —2019 HIPAA Journal

Gaining internal support: TPRM isn't just for IT

The good news is that the conversation around the need for a strong TPRM program is changing. For instance, a mere few years ago if you took your TPRM idea to leadership, a common response was, "We have a BA agreement with every vendor. They're responsible for protecting the data, so we're protected."

Many organizational leaders didn't have enough awareness about acceptable security practices to question how vendors were securing their organization's data once it was outside of their own four walls.

But this mindset and level of awareness has evolved. Today, more and more, fueled by the rampant number, size and frequency of breaches, the conversation sounds like this: "We need to tackle this. What's it going to take and how do we get started?"

Gaining internal support for strengthening your security posture is just the first step. CISOs and IT directors are often tasked with removing some of the organizational barriers that can make it challenging to gain support.

Gaining internal support for strengthening your security posture is just the first step. CISOs and IT directors are often tasked with removing some of the organizational barriers that can make it challenging to gain support. These barriers include a real or perceived lack of resources and internal expertise, as well as a true understanding of your current security program and the security programs of your vendors.

Many organizations believe creation, implementation and maintenance of a TPRM program is strictly an IT responsibility. And while IT can be an integral part of the team, they may not have the full visibility to all the information BAs have access to electronically. And there may even be paper records. An organization needs to know these, too, are being properly handled and secure.

The organization needs to identify everyone internally who has relationships with external vendors to ensure all data is protected. When developing a TPRM program, the security team needs to understand which internal stakeholders need to be included. Does HR hire outside vendors? Does the radiology team hire their own vendors? It is important to know where to look for third parties that are working with your organization. This is often an all-hands-on-deck endeavor and requires enterprise-wide support, including the allocation of resources necessary to create and maintain the program.

Gaining support from various parts of the organization requires targeting the message about the need for a strong security program, especially to supply chain stakeholders. The message must resonate with their areas of accountability and challenges. Let people know the ramifications of a breach on their day-to-day work. Alert them if you've experienced a breach, regardless of whether PHI or PII has been jeopardized or not. Tell them that while the results weren't damaging this time, they may be devastating next time. It's not a scare tactic. It's reality.

Breaches and their remediation can cause public relations nightmares, damage your organization's bottom line and business reputation and temporarily halt vital work processes that adversely impact patient care. And while creating and maintaining a TPRM program can be daunting and requires resources — just ask anyone who's suffered a costly data breach if it's worth the investment.

The five key components of a TPRM program

Though TPRM programs are implemented using various approaches, there are five key components that Intraprise Health believes must be included in any program. These components account for all the parties that need to be involved in any best practices-based TPRM program and speak to the most prominent challenges that affect the healthcare supply chain.

Program Governance

Tiering and Prioritization

Vendor Security Assessment

Vendor Collaboration

Informed Decision-Making

1

Program Governance

Once the decision to implement a TPRM program is agreed upon, Program Governance, or who holds accountability and responsibility for the program, should be clearly defined. Should it be IT? Legal? Compliance? Procurement?

In practice, an argument can be made for any one of a number of possibilities and the right answer will differ from organization to organization. The bottom line is you need an internal champion to build a TPRM program. This champion needs to have unwavering support from the rest of the leadership team.

Governance is often overlooked as a soft, unnecessary objective. It's not. While the rules of engagement between an organization and a BA call for having an information security process in place, and while many BAs believe they have a good one, it can quickly become clear they do not.

Most people who undertake a TPRM process are surprised by how long it takes and how much work it involves. When completed, however, a solid TPRM program and process improves the completion timeframe for vendor assessments, as well as how organizations evaluate third-party risks, leading to greater protection of their data assets.

Intraprise Health's Senior Vice President of Security Services, Brian Parks, recommends the person or department in charge be well-versed in HIPAA, security, privacy and risk management. The governance entity should also be responsible for deciding the need for completing a vendor security risk assessment — typically based on the potential risk the vendor poses to the organization — and making sure the assessment actually gets completed. In many organizations the task of determining the need for an assessment falls to IT, which Parks says is not a good practice, as IT staff don't always have the insight into the full scope of the service the vendor is to provide. In addition, they may not have the knowledge, experience or accountability to ensure a vendor's been fully vetted. An organization must also have a good methodology to thoroughly assess the vendors. An ill-defined process without a clear directive can lead to a lack of complete information, delays, bad assumptions and inaccurate results when it comes to the final assessment.

Program Governance needs to set ground rules and oversee the entire program, cradle to grave. From whom can and should request an assessment to how assessments are completed to the decision-making body that ultimately decides which vendors should be approved, Program Governance needs to oversee the process with specific emphasis on program rules and the decision-making process.

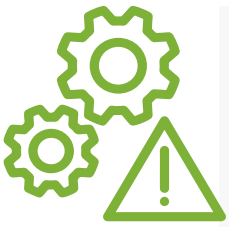
Organizations lacking internal expertise of the TPRM process, which is labor intensive and heavily regulated in healthcare, may want to engage a company specializing in cybersecurity and risk management to help with the process.

Once an organization decides who will build the program, they need to address the other potential challenges that can waylay organizational initiatives — limited finances, lack of staff expertise, time and resources to devote to the program. In addition, many organizations don't maintain a full list of all the contracted vendors with access to your organization's data. Often times, vendor lists reside in various siloed departments and systems.

"Overcoming these obstacles takes leadership, dedication and solid governance," says Parks. "Protecting healthcare organizations' data could be one of the greatest breakthroughs in protecting patient care this century."

Governance includes four foundational elements:

- Obtain board and senior management buy-in: In many cases this will require an educational component, as mentioned above.
- Develop program metrics: These will include key performance indicators and key risk factors.
- Define stakeholder roles and responsibilities: These roles must be fleshed out to include what each person will do through various phases of the program development and implementation.
- Collect recommendations and input from stakeholders before implementation: This will provide valuable insight into structure, roles and responsibilities and other key program factors.[1]



2 Tiering and Prioritization

Critical to a comprehensive TPRM program is the process of categorizing vendor risks.

Vendor risk categorization and prioritization, or tiering, helps an organization strategically quantify the potential risk a vendor could pose to your organization before executing the assessment. Tiers take into account the amount and type of accessibility the vendor has to health information and the physical and technical environment of your healthcare organization, as well as a number of other factors. Tiering helps evaluate how much of a risk a vendor poses to your organization.

Tiering is based on the criteria discovered about a vendor; the security risk assessment is based on this tiering and customized to the type of access the vendor has. Assigning an inherent risk level, or tier, to a vendor application or service will determine the assessment scope as well as the final risk rating assigned upon completion of the third-party assessment.

In an effort to move forward with an engagement, organizations often ask a vendor questions about their security program or pull down a vendor's self-assessment from an assessment library, but don't have the expertise or bandwidth to validate the vendor-provided answers. From a compliance standpoint, then, the basic requirement has been met, box checked. But there is no assurance that the information provided is accurate, and in many most cases, this lack of validation provides virtually no assurance the third party is sufficiently protecting your patient's health information.

In general, a secure third-party vendor has a very mature security program, all of their documents are ready to review when requested and they have assigned security responsibilities in their organization. Achieving a third-party risk certification, such as HITRUST, is also a compelling indicator of a sufficiently secure third-party vendor, though their maintenance of a HITRUST certification needs to be monitored as well as any areas of improvement that have been identified in their certification report.

3

Vendor Security Assessment

A third-party (vendor) security risk assessment (SRA) is the foundation of any TPRM program. The assessment allows your organization to delve deeply with vendors to evaluate their security controls and profile, thereby more specifically assessing the potential risk they pose to your organization.

Part of the security assessment is evidence collection and gathering relevant documentation about the vendor's security program, which could include diagrams, policies and procedures as well as various other forms of evidence. This is followed up with a solid, thoughtful, thorough questionnaire that is customized to the proposed service or product.

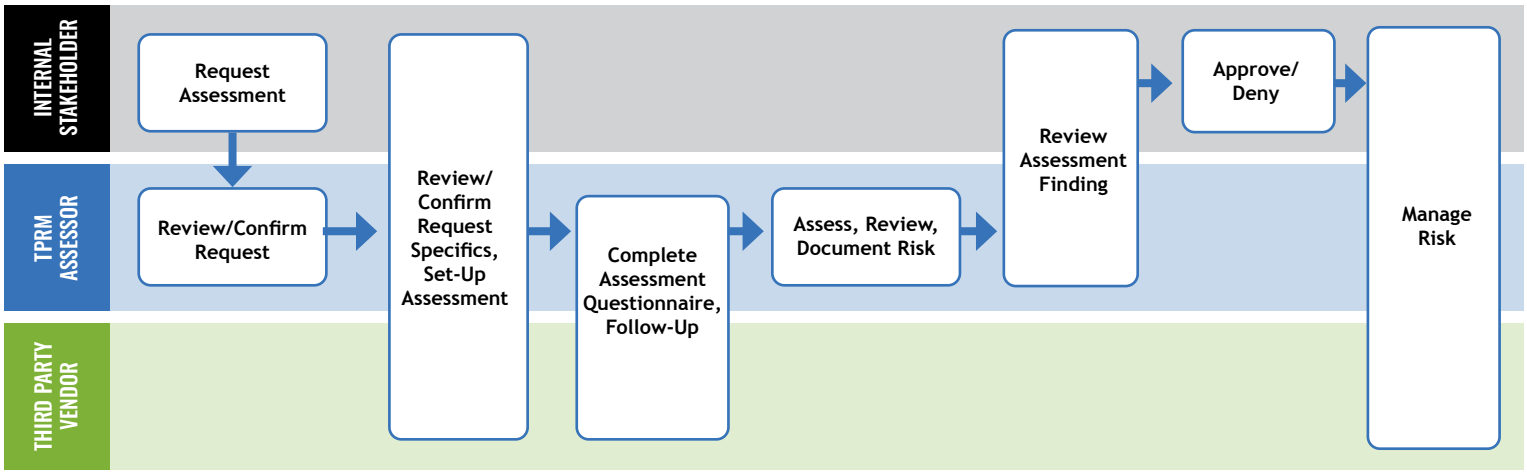
Intraprise Health's Chief Digital Health Officer, Vikas Khosla, says one of the biggest barriers to getting timely and complete information is "throwing a 200- or 300-item questionnaire at the vendor," and asking them to fill it out even if the information requested is overkill or inappropriate for the proposed service or solution. One way to streamline the SRA process is for the organization putting the TPRM in place to utilize insight gained from the tiering process to tailor questions to the vendor during the risk assessment. This will greatly reduce time spent by the vendor responding to questions that don't apply to the product or service they provide the organization. For instance, if a vendor only handles physical records and transmits no electronic data at all, the questions in this part of the process might address the physical facility where records are stored versus their electronic security processes.

Typically the governance person or group identified earlier in the process decides how and when to move forward with a vendor solution or service based on the level and types of risks they are willing to accept.

Building a rapport with vendors by communicating face-to-face or by telephone whenever possible is a good way to expedite some of the assessment process.

It is very important to document all findings, which will typically be shared with an independent decision-making body in the organization (or the organization hired to facilitate the third-party risk management program). Precise and complete information will help these decisionmakers make informed decisions based on the vendors' current security posture.

Typically the governance person or group identified earlier in the process decides how and when to move forward with a vendor solution or service based on the level and types of risks they are willing to accept. An organization may choose to accept the risk, it may require the vendor to remediate the risk, or it may decide not to engage with the vendor. If they decide to move forward, any risks, regardless of severity, must be logged and tracked. This is where many organizations fall short and create greater risk for themselves — by not having a system in place to track and monitor vendor risks on a continuous and recurring basis. An optimized process will have provisions for anyone in the review chain to raise a concern and should allow for open discussion to achieve the desired outcome.



Vendor Collaboration

Forging a mutually respectful and open rapport with the vendor will ensure a smooth process. It's important for vendors to understand the assessment is aimed at improving processes that will eventually benefit their organization as well as yours, thereby making it easier to trust the data security of both organizations. To be transparent about the process, it may be helpful to explain the vendor assessment process by telephone before the process begins. An actual conversation to calibrate expectations and get a real mutual understanding of how the process is going to work, how long it might take and how they could expedite the process is often helpful.

Documenting requests should be very simple and forward-looking and should state expected outcomes as specifically as possible. Make sure you know which person at the vendor organization can provide you with the information you need. Different people may have access to different types of information.

Documenting requests should be very simple and forward-looking and should state expected outcomes as specifically as possible.

The cadence of the review process is important. There's a lot at stake for your healthcare organization as well as the vendors with which you contract, so it's important to communicate with your vendors and stakeholders and keep them up to date with regular progress reporting. When you run into trouble, such as when one of your vendors doesn't get back to you or can't provide something you need in a timely fashion, communicate that, too. Everyone should be continually apprised of the process and your progress.

"This is where the continuous third-party risk management process comes in," Khosla says. "It's not a once-and-done activity."

It's also important to let your vendors know they will be reassessed periodically and they should let you know if any significant changes to their business or their solution occur. Vendor services and technologies change. Vendors release new software, design upgrades, acquire other businesses or are acquired, all of which impacts organizational risk. Updating information on a continuous basis lessens the burden of the re-assessment for everyone.

"Good communication with the vendor throughout the process is vital," Parks adds. "You need a good process to exchange information, ask questions, have them ask questions of you — they're all critical to having a good outcome."

Distilling and compiling the collected information needs to be completed by a qualified and experienced TPRM Assessor. Performing a third-party assessment is different than other internal or technical security assessments. The Assessor needs a good foundation in healthcare compliance and regulatory requirements along with the requisite information and cybersecurity knowledge. The Assessor needs to be able to probe deeper where needed and identify gaps in the third party's security program or areas of non-compliance so they can be clearly communicated to the vendor and decision-makers. The Assessor is responsible for "packaging" the assessment in such a way as to clearly communicate the status, risk rating and gaps to the decision makers so they can make an informed decision about the vendor and their solution.

5

Informed Decision-Making

The third-party assessment process culminates in a solid, informed decision regarding the vendor. Executing on the other key components — Program Governance, Tiering and Prioritization, Vendor Risk Assessment and Vendor Collaboration — paves the way for the decision-making body to have a solid understanding of the service or solution. It also puts the information they need — such as insights, trends, metrics and readily available documentation and reporting — at their fingertips to make the right decisions for the organization.

An independent decision-making body or committee comprised of the appropriate members can ensure that the diverse needs of the business are considered when reviewing and making decisions.

Having the right governance rules in place makes the decision-making process transparent. It allows business owners to understand and be part of the process. It also places the right level of responsibility on the business owner to understand and accept any identified risks. It enables the organization to move forward as one body, all with the same understanding of the solution and the associated risk.

To achieve a strong outcome organizations should start with gathering the important information up front. The assessment report, itself, should be concise, but contain all the information needed by the committee. It's a good idea to also have an executive-level status indicator (i.e. color coding) or a risk rating so that the reader gets a quick understanding of the findings and the vendor's assessed level of compliance. Decisions can come either via committee meetings or via electronic collaboration (email, a workflow system, Microsoft Teams, etc.). It should not be a cumbersome process. If you have a good report with risks clearly outlined, the decisionmakers can quickly and easily evaluate the results in the vast majority of assessments.

Software TPRM platforms in the market

Many organizations, especially in highly regulated industries such as healthcare, have started implementing TPRM programs, often times through a patchwork approach using manual processes and other documentation tools such as MS Excel and Word. To provide greater automation and scalability, software/services companies are developing solutions to replace or supplement the patchwork approach of early TPRM programs. We have looked at the sector broadly and summarized the different categories of software products found in the market currently.

Web Scanners

Technical scanners scale well though they focus solely on technical security, usually considering only the web-facing technology (via scans and crawlers), but don't holistically assess the full security program. They are very good at understanding if the vendor's solution, either hosted in their data center or provided as a cloud service, has any known technical vulnerabilities or uses open source code/apps.

These types of software products are similar to security scanners that provide some additional vulnerability and penetration testing capabilities. However, these tools do not assess security practices, cybersecurity controls or regulatory compliance. One cannot get a true sense of the vendor's security program and implemented controls, or more importantly, the gaps that may exist. Nonetheless, they are a good complement to a TPRM assessment specifically as it relates to technical vulnerabilities for those companies that seem weak in this area.

Shrink wrapped Solutions

"Shrink wrapped" or out-of-the-box solutions typically are industry agnostic, horizontal solutions that provide a pre-defined TPRM process. They provide some needed tools to help automate workflows, track and monitor, but do not adapt to individual organizational processes and do not address governance rules or healthcare-specific regulations. These are software-only solutions that do not provide validation or process outsourcing options. They also tend to be more broad than deep in terms of their feature sets. They are good for process tracking, often times with connectors to popular help desk ticketing software products but with limited workflow configuration, rules, collaboration, analytics and visualization capabilities.

GRC software

Governance, risk and compliance (GRC) tools can manage an organization's overall governance, enterprise risk management and regulatory compliance programs. Popular in many large enterprises, GRC software requires implementation along with ongoing system administration, configuration and support. Typically, there are some number of full-time equivalents, or FTEs, that are dedicated to managing, configuring, operating and supporting the system so the organization can continue to receive ongoing value from the product. TPRM automation is usually offered modularly, requiring a "build-out" to adapt to an enterprise's processes and workflows.

Sometimes organizations seeking to automate their TPRM program are concerned because they already have a GRC tool in place. However, a good security risk management platform will complement the existing GRC system, not replace it; it can be integrated, thereby saving time and resources while improving efficiency and security. Gartner published an in-depth paper on the future of GRC tools and presents a model whereby the different aspects of a security program, including vendor risk management, are connected across a continuum called Integrated Risk Management (IRM).[2] As the industry evolves further to a more IRM-based approach to managing governance, risk and compliance organizations are finding greater value and utility by "plugging in" purpose-built security solutions, such as TPRM, into their GRC product.

How to execute a strong TPRM program in your healthcare organization

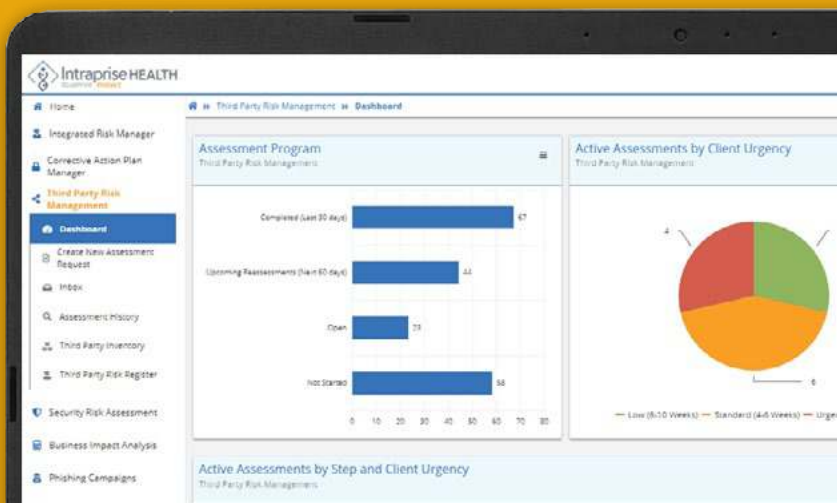
- ✔ Armed with facts about the need for a comprehensive TPRM program, rally internal organizational support for a TPRM program by targeting messages about security and its impact to various organizational units.
- ✔ Incorporate these five key components into your program: Governance, Tiering and Prioritization, Vendor Security Assessment, Vendor Collaboration and Informed Decision-Making.
- ✔ Once the decision to pursue a program is made, determine the governance and scope of the process and develop policies and timelines for key activities.
- ✔ Develop a solid, thoughtful and thorough questionnaire customized to the proposed vendor service or utilize a TPRM program automation solution.
- ✔ Employ a validation component that provides greater assurance for your program.
- ✔ Adhere to the governance rules and processes, collect evidence about your third-party vendors and the risks they pose to the organization.
- ✔ Communicate clearly and frequently with vendors so you will be able to collect good data.
- ✔ Interview key vendor personnel to collect needed information and seek clarification.
- ✔ Once evidence is collected, distill it and present a meaningful and easy-to-read report back to organizational stakeholders.
- ✔ Document, monitor and follow up on gaps in vendor security.
- ✔ Reassess vendors on a scheduled basis and when conditions change.
- ✔ Seek out the right subject matter expertise to operate your program.

BluePrint Protect™

Intraprise Health's BluePrint Protect solution provides CISOs with a single pane of glass view of their TPRM program. Users can automate their program with scalable, intelligent automation and collaboration features with drill-down, real-time dashboards that provide a clear view of vendor risk management. Designed by healthcare security experts who actually use the software, BluePrint Protect gives users the tools to automate TPRM workflows, apply intelligent rules, collaborate with all stakeholders, identify, report on and remediate enterprise vendor security risks — all in one place.

BluePrint Protect's TPRM module starts with two important factors to any assessment, profiling and tiering, to identify the type and number of questions a vendor will receive to gauge the inherent or potential level of risk that is specific to that vendor. The profiling form collects information from the customer stakeholders and third-party teams to identify the full scope of services, application technology and system access required to deliver their offering to the customer. In turn a dynamic, online assessment questionnaire is generated based on the responses to the profile form and tier level.

Using Protect, third parties respond to the tailored assessment questions. Once complete, Intraprise Health's certified security experts work within the application to evaluate each third party's responses and supporting documentation to validate the assessment. A project risk rating is assigned and a system-generated report is created for the decision-making committee. Having a team of security experts take the extra step to make sure the assessment responses are accurate and supported by the documentation is a key differentiator because of the validation and assurance this provides.



Find out more about BluePrint Protect™ .

Conclusion

In an era of increased fines, shifting priorities, breaches, ransomware and the rising value of health care data, CISOs and CIOs are evolving their enterprise security programs towards a risk management approach and third-party risk management is a critical element.

The HIPAA requirement to properly handle data, plus the skyrocketing costs of breaches from third parties (and fourth and fifth parties!), as well as the less easily quantifiable risks to an organization's reputation, make third party risk an area of increasing concern.

Third parties are a major risk factor that must be understood, assessed, remediated and monitored on an ongoing basis. Understanding the elements to a strong TPRM program, and how to implement them will help healthcare organizations take control of the risks they face and result in a stronger, more secure organization.

[1] https://sharedassessments.org/blog/building-your-tprm-program-part-1-four-foundational-steps-to-build-your-third-party-risk-management-program-on/

[2] https://blogs.gartner.com/john-wheeler/why-leading-software-vendors-are-dumping-grc-for-irm-2/