SecZetta™

THE RISK MANAGEMENT BLIND SPOT

Third-Party Identities Often Create Unrecognized Risks

Introduction

An ever-growing area of concentration in risk management is identifying and mitigating the risks that third parties introduce to an organization – and perhaps equally important, ensuring that third parties don't introduce unmeasured risk. One might think that third-party governance systems, sometimes used for vendor assessments, could be used to manage the identity and access management aspects of the vendor relationship. However, most security vendors do not consider identity to be part of third-party management. In fact, organizations realize the risk of third parties the moment they provision access, whether or not it is measured, mitigated, or even known.

Today it's common practice for risk management teams to assess a third party's risk controls by evaluating responses to a Standardized Information Gathering (SIG) questionnaire. Unfortunately, these vendor security assessments based on SIG answers may give the organization false confidence in a vendor's actual security posture, when in fact the assessments:

- Are fairly superficial because they rely on an honest, accurate response from the vendor
- Focus only on the vendor organization's practices which results in a risk management blind spot for risks related to the vendor's users who access organization resources

In addition, onboarding processes are usually automated for employees but are highly manual for third-party users. While not ideal, manual processes may meet the minimum needs of smaller organizations. However, for larger or highly regulated organizations, these manual processes are time-consuming, costly, error-prone, and expand the potential for additional risk associated with third-party users.

To effectively manage third-party risk, these organizations require a purpose-built, scalable solution that improves the granularity, transparency, consistency, and agility of their third-party risk management program.

Risk Management Best Practices

Before a risk can be properly managed, risk management teams must understand which risks the organization considers to be acceptable so the manager can take action if risk exceeds acceptable limits. Each organization is somewhat unique in how it defines acceptable risk and ensure that each risk remains within an acceptable range. Many organizations consider acceptable risk on at least two levels: the organization level (risk appetite) and a granular level (risk tolerance).

Risk Appetite

Risk appetite is "the level of risk the group is willing to take to achieve strategic objectives," according to a paper on risk appetite statements by the Institute for Risk Management (IRM). Risk appetite is sometimes communicated through an organization-level risk appetite statement that has been approved by the highest levels of an organization. Analyst firm Gartner identifies risk appetite statements as the top security and risk trend for 2020. "Leading SRM (Security and Risk Management) leaders are creating pragmatic risk appetite statements linked to business outcomes to engage their stakeholders more effectively," Gartner noted.

Coined by the IRM as an "increasingly useful concept," risk appetite should in theory impact an organization's approach to all risk including information security risk.

According to the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the three key questions to ask to create a risk appetite statement are (paraphrased):

- Which risks will the organization reject (not accept)? (e.g. quality compromises)
- Which risks will the organization accept to take on new initiatives? (e.g. new product lines)
- Which risks will the organization accept for competing objectives? (e.g. gross profit vs. market share?)

In Building a Federal Risk Appetite Framework, Deloitte provides a Risk Appetite Scale example with five risk profiles ranging from Risk Seeking to Risk Averse. The profile type impacts risk response.

The risk management team interprets the risk appetite statement, when available, to make risk-intelligent decisions that fall within the organization's risk appetite.

Risk Tolerance

Armed with an approved risk appetite statement, the risk management team can develop associated metrics to monitor risk management effectiveness and prioritize and respond to risk at a more granular level. This includes risks posed by third parties and their users.

The clearest definition of risk tolerance may be from ISO Guide 73: 2009 Risk Management – Vocabulary: "an organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives." In practice, risk tolerance typically involves establishing processes for assigning risk levels and accepting risk.

To establish risk tolerance, the risk management team considers factors such as:

- Management guidance including the risk appetite statement
- Compliance concerns
- Privacy risks
- Security threats that impact confidentiality, integrity, or availability
- Value of data and assets accessed
- Industry and competitive pressure

For third-party risk management, risk tolerances should be established for both the vendor organization and the vendor's users, as described below.

Applying Risk Tolerance for Third Parties

Vendor Risk Tolerance

Before a contract is signed and at a regular frequency thereafter, client organizations typically conduct an assessment to review a vendor's security maturity. The client typically sends the vendor a SIG questionnaire as an email attachment which the vendor completes and returns. The questionnaire outlines high-level security requirements and attempts to identify areas where the vendor may fall short. Clients often take the vendor answers at face value and do not request documented evidence of implementation such as policies, procedures, or screenshots.

Any identified security shortcomings should be addressed to reduce risk through one or more mitigation methods such as transferring risk (example: insurance), sharing risk (example: sharing risk with a vendor), or implementing layered, preventative, detective, corrective, and/or compensating controls. Residual risk, which is risk remaining after mitigation, should be formally accepted through an exception process.

The result of the vendor risk assessment is typically a simple pass/fail decision, a gating step in an overall vendor onboarding process that also includes price negotiations and Legal review. While potentially informative at a high level, vendor risk assessments can be matured to ensure appropriate controls and workflows are selected based on risk tolerance.

In part, the risk management team should consider establishing risk ratings (typically critical, high, medium, and low or CHML) with risk and acceptance criteria for each rating. The vendor rating is assigned after any mitigation.

For example, an organization with a moderately risk-averse risk appetite could specify that:

- A critical rating is considered a failure; a critical-rated vendor cannot be approved.
- A vendor with a high rating can be accepted via an exception approved by the top Information Security leader.
- A vendor with a medium rating can be accepted via an exception approved by the control or business owner.
- A low-risk vendor is accepted and approved by default, based on the risk management team's determination that the vendor poses minimal risk.

In addition, review cycle frequencies can be established based on the risk rating, so that higher-risk vendors are reviewed more often.

Each rating should also have criteria that can be applied objectively so that multiple people can apply the criteria and arrive at the same rating.

All key risks should also be entered into a risk register or catalog to ensure periodic review and acceptance. A risk register may also include exceptions, which usually have an expiration date and must be renewed.

User-Level Risk Tolerance

After the vendor organization passes the information security assessment, the risk management team typically considers their work done and hands off the relationship to the line of business. This is not enough.

Ideally, as part of the risk assessment or as a subsequent process, the company would establish user risk ratings (again, typically using the CHML schema) that others can apply to clearly determine whether the risk each user poses falls within the organization's risk tolerance. After all, "you can't manage what you don't measure," as the saying goes.

Just as we saw for vendor-level risk, the risk management team can establish risk and acceptance criteria for each user risk rating.

Mature organizations collect comprehensive, contextual information for user risk ratings such as:

- The risk rating of the user's organization – Note: the user's rating should never be lower than the organization's rating
- User location
- Role within the organization
- Department of the user's sponsor or delegate
- Industry
- Identity validations (credentials, licenses, security clearance levels, skillsets)
- Access to be granted based on role/relationship
- Sensitivity of facilities, systems, and data being accessed
- Work history

The more relevant and complete the rating information, the more informed the risk decision.

The risk rating can be used to trigger workflows. For example, an organization with a moderately risk averse appetite could build third-party onboarding and recertification workflows that:

- Reject all users that have a critical rating.
- Allow a high-risk user via an exception approved by the top Information Security leader.
- Allow a medium-risk user via an exception approved by the control or business owner.
- Automatically approve access for all low-risk users.

This level of control would be impossible to achieve with manual processes. Manual processes increase the likelihood of inconsistencies that result in orphaned accounts, excessive privileges, and segregation of duties violations – problems that can in turn lead to data breaches, data integrity problems, and poor system performance. Automation of onboarding processes reduces errors, decreases process labor costs, avoids opportunity costs, and accelerates the provisioning and deprovisioning of credentials and access. Active, automated management of third-party identities involves continuously validating the current business need for access.

Organizations have seen unsatisfactory levels of success in the following:

- An expensive homegrown system or a complex integration requiring data feeds to get systems communicating
- Expensive customization of existing Human Resources (HR), Identity and Access Management (IAM), Identity Governance and Administration (IGA), Vendor Management Systems, and other systems.
- Therefore, automated third-party identity risk management can be achieved only by implementing a purpose-built, third-party identity risk tool, designed to rate risk at both the vendor and user levels.

Third-Party Identity Risk Management Responsibilities

The Chief Risk Officer (CRO) is usually responsible for identifying, monitoring, and mitigating internal and external risks. In practice, third-party identities are often loosely managed via ad hoc processes, sometimes involving a collection of spreadsheets, databases, and tools. Many CROs share the burden of managing these identities with other teams and stakeholders that are not well equipped to manage risk, such as:

- Human Resources: Centralized and focused on managing full-time employees.
- Procurement: Focused on managing contracts.
- IT: Focused on managing technology assets and access to assets.

Sometimes, onboarding and account recertification responsibilities fall to separate teams. The HR team handles onboarding, while account recertification may be handled by IT. The CRO may have limited visibility into the activity of other teams.

Understandably, problems with the management of third-party identities are common during information security certification audits such as ISO 27001 or HITRUST.

The primary responsibility for approving third-party identities falls to the leader closest to the work effort, who can validate the ongoing need for access – the user's internal manager or the vendor sponsor – while the CRO maintains visibility.

Complex workflows, for instance those involving external approvers or multiple internal approvers, benefit from automation and a holistic approach that combines identity risk and identity lifecycle with an access management program.

SecZetta's Approach to Third-Party Identity Management

If your organization needs to better manage the risks associated with third-party users, SecZetta can help. Our Third-Party Identity Risk Management solution provides a comprehensive set of capabilities that help organizations improve operational efficiency and reduce the cost and risk of managing third-party identities.

SecZetta's solution does this by allowing an organization to streamline third-party identity management and risk rate, consolidate, store, and validate third-party identities.

SecZetta's solution uniquely offers:

- An external facing collaboration hub that enables third-party users and their internal sponsors to provide key data needed for onboarding and throughout the lifecycle of the user. Identity sponsors established based on the type of relationship a user has with an organization.
- Conditional workflows for every type of non-employee (such as independent contractors, consultants, freelancers, partners, vendors, students, physicians, volunteers, and customers) which can be used to collect pertinent identity information including signed documents such as non-disclosure agreements and acceptable use policies and to notify approvers.
- The ability to establish risk ratings for both third parties and their users.
- User risk ratings that can be dynamically adjusted to reflect temporary or permanent changes to risk tolerances.
- Quickly adjusted user privileges based on emerging threats such as restricting access to previously approved areas based on a physical threat.
- The merging of duplicate accounts into a master identity that displays the most important and current information first.
- Storage of consolidated information in an identity directory to provide global identity visibility and management.
- Identity revalidation workflows, initiated at a desired frequency and involving as many internal and external approvers and stakeholders as desired, to avoid untimely removal of access and orphaned accounts.
- Identification of fourth party/"nth party" accounts for monitoring purposes when the client organization might not have contractual rights to audit.
- Specialized use case support for industries, M&A, and non-human identities including bots, service accounts, and IoT devices.

Conclusion

Risk management teams can best ensure that third-party risk falls within established risk tolerances by aligning tolerances with an organizational-level risk appetite statement and implementing risk ratings at the vendor and user levels. Workflows can then be built and executed based on the rating, user type, or other factors.

For larger organizations, third-party identity management needs go beyond what can be readily managed with manual workflows, homegrown software, or customized systems. Inconsistency from poorly designed workflows results in overlooked risk, discovered during audits or security incidents.

SecZetta's Third-party Identity Risk Management solution manages risk at the user level while incorporating vendor risk. By utilizing the SecZetta solution, organizations are improving the quality of risk management while at the same time using automation to make workflows simpler and more efficient. Such automation is essential because it creates consistency, limits human error, and avoids risky delays in the removal of access.

With the SecZetta's Third-party Identity Risk Management solution, automated and proactive workflows ensure process compliance, data integrity, and timely access changes to reduce and eliminate third-party identity risk.

About SecZetta

SecZetta sets the standard for managing non-employee risks and identities.

SecZetta is the leading provider of third-party identity management solutions. Our solutions enable organizations to execute risk-based identity access and identity lifecycle strategies for diverse non-employee populations. Because the solution suite is purpose-built, it's uniquely able to manage the complex relationships organizations have with non-employees in a single, easy-to-use application that simultaneously helps facilitate commercial initiatives, support regulatory compliance, and reduce third-party risk. For more information visit, https://seczetta.com/.