Third-Party Identity Maturity Assessment

SecZetta

Your SecZetta Identity Maturity Assessment

Congratulations! You have successfully completed the SecZetta Third-Party, Non-Employee Identity Program Maturity Survey.

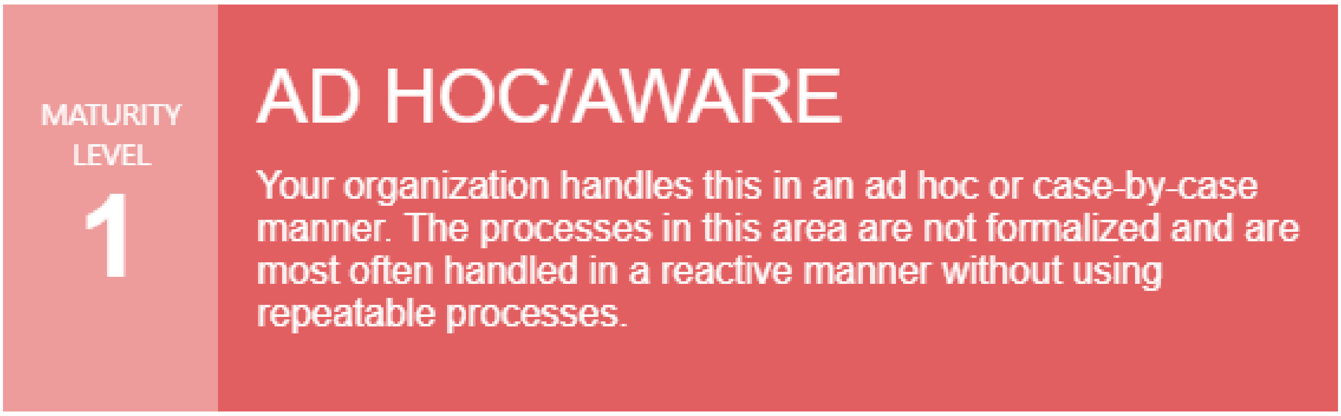
EVALUATION: RISK MATURITY LEVEL

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.

Your organization's potential risk of an audit/compliance violation and ultimately the threat of a third-party data breach are dependent on the processes your organization currently have in place to identify and mitigate third-party threats.

YOUR ASSESSMENT

Your current risk maturity level indicates you're at a higher risk of experiencing a failed audit, a hefty fine for not meeting regulatory or compliance mandates and are at an increased risk of a third-party data breach. Your ad hoc approach to third-party identity risk management can be improved upon by adopting a “risk-first” mindset that integrates cybersecurity, compliance, identity management, and risk governance to proactively manage the full lifecycle of your non-employees.



MATURITY LEVEL 1

AD HOC/AWARE

Your organization handles this in an ad hoc or case-by-case manner. The processes in this area are not formalized and are most often handled in a reactive manner without using repeatable processes.

IMPROVING YOUR MATURITY

We know you're keen on decreasing your organization's risk by improving your third-party, non-employee identity program. To better secure your organization's assets and improve business efficiencies, we recommend the following resources to help guide you to the next level of maturity.

The Identity Gap in Third-Party Risk Management

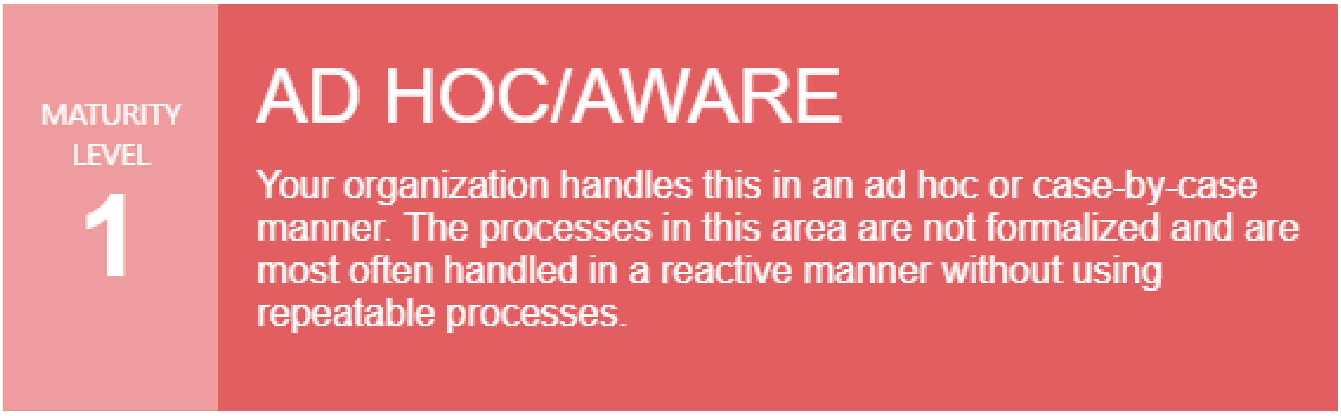
Gartner Market Guide on Insider Risk Management Solutions

EVALUATION: ENABLEMENT MATURITY LEVEL

This is an assessment of your organization's ability to utilize third-party user identity data to address the complex requirements necessary to effectively govern access. Ultimately, more comprehensive knowledge of non-employees can help optimize their contribution to the overall success of your organization. From a business process enablement and risk mitigation perspective, this knowledge is essential in making decisions to grant and remove access to an organization's systems in a timely and accurate manner.

YOUR ASSESSMENT

Your current Enablement maturity level indicates large gaps in your third-party identity risk management processes. Your current approach to gathering non-employee data and managing the information is inefficient, costly, and often prone to error. This ad hoc approach to third-party identity risk management can be improved upon by applying as much rigor to your processes for non-employees as are applied for your employees.



MATURITY LEVEL 1

AD HOC/AWARE

Your organization handles this in an ad hoc or case-by-case manner. The processes in this area are not formalized and are most often handled in a reactive manner without using repeatable processes.

IMPROVING YOUR MATURITY

We're sure you're keen on improving your organization's third-party, non-employee identity program. To better secure your organizations assets and improve business efficiencies, we recommend the following resources to help guide you to the next level of maturity.

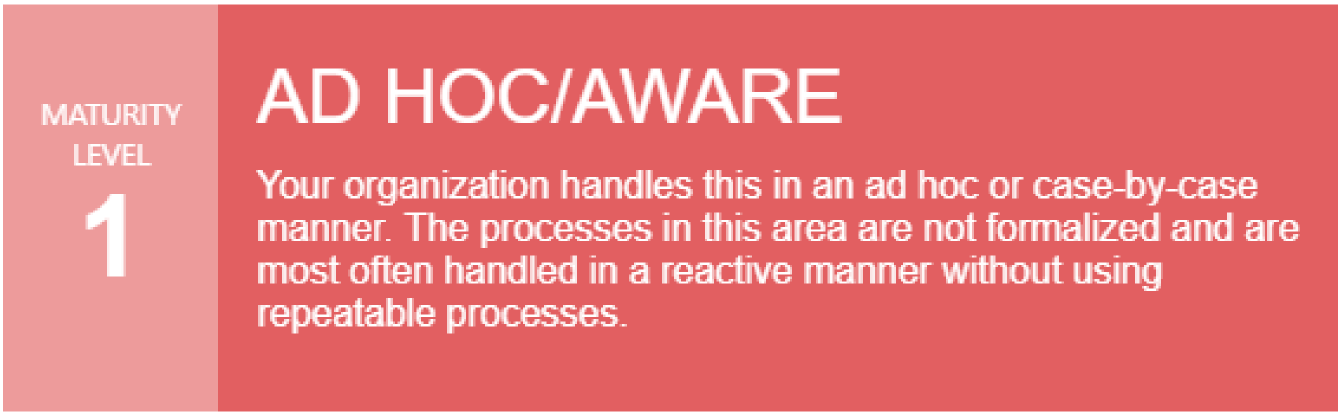
Non-Employee Lifecycle Management Pictogram with SecZetta

EVALUATION: AUTOMATION MATURITY LEVEL

This is an assessment of your organization's overall operational efficiency in executing risk-based identity and lifecycle strategies for diverse third-party user populations. Ideally, your company is utilizing automated workflows for complete transparency into the dynamic relationships they have with each individual third-party identity and are thus able to make well-informed, risk-based decisions about provisioning, verifying, and deprovisioning access.

YOUR ASSESSMENT

Your current Automation maturity level indicates large scale inefficiencies, financial waste, and a process prone to human error in managing third-party, non-employee identities. Your current ad hoc approach to onboarding, auditing, verification, and the removal of access upon termination lack a centralized or complete approach that is exposing your organization to unnecessary risks.



MATURITY LEVEL 1

AD HOC/AWARE

Your organization handles this in an ad hoc or case-by-case manner. The processes in this area are not formalized and are most often handled in a reactive manner without using repeatable processes.

IMPROVING YOUR MATURITY

We're sure you're keen on improving your organization's third-party, non-employee identity program. To better secure your organizations assets and improve business efficiencies, we recommend the following resources to help guide you to the next level of maturity.

The Missing Link to “Mastering” a Modern Identity Program

Evolution of Identity, The (ID) Proof of Risk

SecZetta and Human Resource Management Systems: Better Together!

Your Organization's Overall Risk of Experiencing a Third-Party Breach Based on the Maturity of Your Identity Program

Below is an indicator of your overall risk of experiencing a third-party breach based on your organization's current third-party identity maturity level. This assessment is a good gauge of your organizations current ability to manage third-party identities, govern non-employee access, and the impact your current processes have on preventing a breach.

Have a question?

If you have a question about this assessment or need additional details on how SecZetta can work with your organization to reduce the risk of a third-party breach through a robust third-party identity risk management solution, please contact us or call +1.781.832.0767 us to discuss.

Contact Us

Thank You

Thank you for completing the SecZetta Third-Party, Non-Employee Identity Program Maturity Survey. We have sent you an email with the report.

Response Summary

Basic Details

	Question	Your Response
2	Country	United States
3	Industry	Energy
4	Size of company or government agency	5,000-9,999
5	Job title	Director of IT/IAM

6. How many third-party non-employees (partners, vendors, freelancers, etc.) are being provided access to your facilities, systems, and data?

		Your Response
	Less than 250	
	250-999	
	1,000-2,499	
	2,500-4,999	
	5,000-9,999	✓
	10,000+	

7. What is your confidence level in the accuracy of this data?

		Your Response
	High	
	Medium	✓
	Low	
	I don't know	

8. What types of "third party" non-employees are being provided access to your facilities, systems, and data?

		Your Response
	Affiliates	✓
	Agents	
	Clinical workers	
	Consultants	✓
	Contingent Workers	✓

	Contractors	✓
	Freelancers	
	Interns	
	Partners	✓
	Researchers	✓
	Seasonal workers	
	Students/Alumni	
	Supply Chain	✓
	Vendors	✓
	Volunteers	

9. Has your company suffered a security incident related to third-party user access?

		Your Response
	I don't know	✓
	No	
	Yes	

10. Do you include non-human workers like Bots, IoT devices, RPA in your "third party" population types?

		Your Response
	No	
	No, but we do have defined lifecycle and risk processes for non-human workers	✓
	Yes, and our lifecycle and risk processes are similar	

11. Select from the following business functions that are involved in the management and maintenance of third-party non-employees.

		Your Response
	GRC Team	✓
	HR	✓
	IT	✓
	Legal	✓
	Line of business	✓
	Procurement	✓
	Sponsor	

		✓

12. Where does the most complete, authoritative information for your third-party non-employees reside?

		Your Response
	Active directory or similar	
	IAM/IGA solution	✓
	HR Information System (e.g., Workday, SAP, etc.)	
	SecZetta	
	Spreadsheets or similar	
	Vendor Management System (VMS)	
	IT Service Management system (ServiceNow, Remedy, etc.)	
	Homegrown or proprietary system	
	Disparate across multiple systems	
	I don't know	

13. How reliable, current, and well-maintained is this "non employee" information?

		Your Response
	Very reliable when onboarded and proactively maintained thereafter	
	Reliable when onboarded but minimally maintained thereafter	✓
	Not particularly reliable (e.g, often incomplete and frequent data entry errors)	
	No defined or reliable authoritative source repository	

14. How does your third-party vendor participate in the onboarding of its employees for access to your systems?

		Your Response
	Internal sponsor coordinates information gathering via email or phone and manually creates request	
	Vendor submits a form or other structured data via email, ticket, or similar that is used to trigger onboarding	✓
	Vendor delegate has access and contributes directly to our authoritative source	
	Vendors have direct integration with our active directory or similar	

15. Have you had audit findings related to third parties in the past?

		Your Response
	Yes	✓
	No	

16. How do you prove that your "third-party" non-employees are who they say they are?

		Your Response
	"In person verification" via government ID or similar	✓
	Digital identity proofing	
	Neither in-person nor digital identity proofing, but we do use strong authentication for access (e.g., MFA)	
	We don't confirm this information	
	I don't know	

17. How are third-party non-employees offboarded?

		Your Response
	Automated process via integration with authoritative source	
	Pre-defined access expiration date	
	Manual requests through IT	✓
	Via account activity /last login	
	They are not offboarded in a consistent way	
	I don't know	

18. How well-defined are the identity lifecycle and risk processes for your "third party" population types?

		Your Response
	Not Done	
	Ad Hoc	
	Progressing	✓
	Mature	
	Mastered	

19. How does your organization assess risk for new third-party relationships?

		Your Response
	Not Done	
	Ad Hoc	
	Progressing	✓
	Mature	
	Mastered	

20. How does your organization use third-party risk data to inform decisions about third-party access and revalidation?

		Your Response
	Not Done	✓
	Ad Hoc	
	Progressing	
	Mature	
	Mastered	

21. How does your organization meet third-party legal & regulatory requirements (CCPA, GDPR, ...) for your information security program?

		Your Response
	Not Done	
	Ad Hoc	✓
	Progressing	
	Mature	
	Mastered	

22. How does your organization conduct identity proofing for "third party" non-employees who are granted access to facilities, systems, or data?

		Your Response
	Not Done	
	Ad Hoc	
	Progressing	
	Mature	✓
	Mastered	

23. How does your organization automate the onboarding of "third party" non-employees who are granted access to facilities, systems, or data?

		Your Response
	Not Done	
	Ad Hoc	
	Progressing	
	Mature	✓
	Mastered	

24. How does your organization automate the offboarding, including access removal, for "third party" non-employees?

		Your Response
	Not Done	
	Ad Hoc	
	Progressing	✓
	Mature	
	Mastered	

25. How does your organization revalidate your third-party non-employees' profile and status?

		Your Response
	Not Done	
	Ad Hoc	
	Progressing	✓
	Mature	
	Mastered	

If you need assistance understanding the results of your assessment or are interested in improving your organization's identity management processes to better secure your data, contact ZecZetta to learn more.

Contact SecZetta