North Dakota

NORTH Dakota
Be Legendary.

North Dakota Information Technology and
Office of Management and Budget

Business Process Innovations

"Guardians of Trust: ND's Third-Party Risk Management Initiative"

July 1, 2023

Alisa Cook (acook@nd.gov)

Executive Summary

In response to the evolving landscape of cloud technologies to safeguard citizen data, North Dakota (ND) has implemented a robust Third-Party Risk Management program. This initiative addresses the inherent security risks associated with third-party vendors by conducting thorough assessments prior to contract execution and maintaining continuous monitoring throughout the vendor relationship lifecycle. Leveraging automated workflows and strategic partnerships, NDIT has established a scalable framework that enhances security and also upholds the state's commitment to citizen trust and data protection.

IDEA:

What problem or opportunity does the project address?

The Third-Party Risk Management (TPRM) program addresses the critical challenge of securing state data amid the rapid shift towards cloud technology procurement. As North Dakota increasingly relies on cloud solutions to enhance efficiencies for agencies and citizens, the state faces reduced control over hosting configurations essential for securing data in transit and at rest. This transformation necessitates a robust mechanism to ensure the protection of citizen data, a responsibility that the TPRM program effectively fulfills.

The TPRM program mitigates security concerns by proactively identifying potential risks before entering into contracts with vendors. This preemptive approach ensures only those vendors who meet stringent security standards are engaged, thereby safeguarding state data from the outset. Moreover, the program continuously monitors the security performance of these vendors throughout the lifecycle of their systems, providing ongoing assurance of data protection.

By implementing the TPRM program, North Dakota strengthens its moral and ethical commitment to protecting citizen data. This formal and thorough security review process of vendor practices significantly reduces the risk of data breaches, ensuring citizen information remains secure. Consequently, the program not only addresses a critical business problem but also enhances business processes and increases citizen trust and engagement with state government.

Why does it matter?

Addressing the problem of third-party risk management is crucial for North Dakota as the state embraces a cloud-first strategy to enhance service delivery and operational efficiencies. The TPRM program ensures that while the state leverages the benefits of cloud technologies, it does not compromise the security of citizen data. This program is essential in identifying potential risks before contracts are signed with vendors and continuously monitoring their security performance, thereby safeguarding sensitive information and maintaining system availability for essential services.

The business rationale for implementing the TPRM program includes mitigating the reputational and financial risks associated with potential security incidents involving cloud providers. By proactively identifying and addressing vulnerabilities, the state avoids the substantial costs associated with data

breaches, such as data recovery, legal fees, fines, and loss of public trust. Continuous monitoring of vendor security performance ensures emerging threats are promptly identified and mitigated, reducing the potential for financial losses and maintaining the integrity of state operations.

The program also strengthens North Dakota's commitment to protecting its citizens' data and fostering trust in state services. Human resources dedicated to the TPRM program conduct thorough security assessments and implement necessary measures, ensuring control over data security even when hosted by third-party providers. By maintaining robust data protection, the state enhances public confidence in its digital services, encouraging greater engagement and utilization. In essence, the TPRM program is a strategic investment that secures citizen data, maintains public trust, and supports reliable digital governance.

What makes it different?

The third-party risk management (TPRM) program in North Dakota stands out due to its innovative approach to automating workflows and streamlining vendor assessments. NDIT administers the program through a custom-built application that classifies vendors based on availability needs and data sensitivity, allowing for tailored risk assessments. The dynamic questionnaire within the application ensures the right questions are asked at the right time, enhancing the accuracy and efficiency of vendor due diligence.

Moreover, the TPRM program goes beyond initial assessments by implementing continuous monitoring throughout the lifecycle of vendor contracts. Automated alerts notify NDIT of any significant drops in vendor security scores, enabling timely intervention to mitigate emerging risks. This proactive monitoring approach ensures ongoing compliance and security, safeguarding citizen data and maintaining operational resilience.

Furthermore, the partnership with StateRAMP adds another layer of efficiency and effectiveness to the TPRM program. By leveraging StateRAMP's expertise and continuous monitoring capabilities for vendors that are StateRAMP authorized, North Dakota enhances its ability to vet vendor security controls and uphold rigorous standards of data protection. This collaborative approach is the state's commitment to innovation, security, and effective risk management in the procurement of cloud technologies.

What makes it universal?

The third-party risk management (TPRM) program in North Dakota addresses a universal challenge faced by all states when utilizing cloud services. As cloud adoption becomes increasingly prevalent across the public sector, ensuring the security and integrity of data shared with third-party vendors is paramount. N.D.'s TPRM program serves as a model for other states, offering insights into the creation, implementation, and measurement of success in managing third-party risks.

Furthermore, the inclusion of fast-track pathways for vendors with FedRAMP, StateRAMP, or HITRUST authorization showcases the program's universal applicability. By leveraging established security frameworks such as StateRAMP, North Dakota enhances efficiency and reduces duplication of efforts for vendors seeking authorization across multiple states. This collaborative approach streamlines the

assessment process for vendors and also aligns with the State CIO Top Ten Priorities, particularly in cybersecurity and risk management, governance, and resource optimization.

Overall, the TPRM program's universal relevance lies in its ability to address common challenges faced by states in managing third-party risks associated with cloud technologies. By implementing robust assessment processes and leveraging partnerships with recognized security frameworks, North Dakota sets a precedent for effective risk management that can be adopted and adapted by states nationwide.

Implementation

What was the roadmap?

The roadmap for the third-party risk management (TPRM) program began with securing funding in late 2020 to implement a comprehensive risk management strategy. The initial focus was on implementing TPRM for the Executive branch agencies, with the aim of identifying and mitigating risks associated with third-party vendors before entering into contracts. This required close collaboration between the North Dakota Information Technology (NDIT) and the Office of Management and Budget (OMB), as procurement activities are managed by OMB.

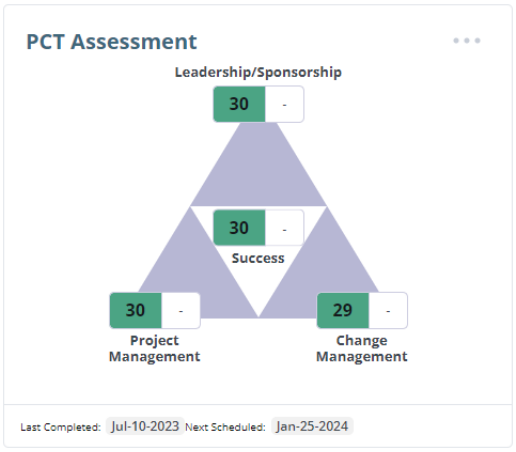
To ensure successful implementation, NDIT developed a change management plan over two years, which involved training agencies, procurement officers, vendors, and key IT staff involved in the third-party assessment process. On July 1, 2023, NDIT and OMB officially mandated, through policy, that any new third-party vendor hosting state data or having administrative access to NDIT systems undergo a third-party assessment. Additionally, existing vendors up for renewal were also required to undergo assessment, ensuring continuous risk management throughout vendor partnerships. This project aligns with an enterprise view by integrating risk management practices into procurement processes, safeguarding state data, and enhancing overall security posture. The project management approach involved close collaboration between NDIT, OMB, agencies, procurement officers, and vendors to ensure clear communication, training, and policy enforcement.

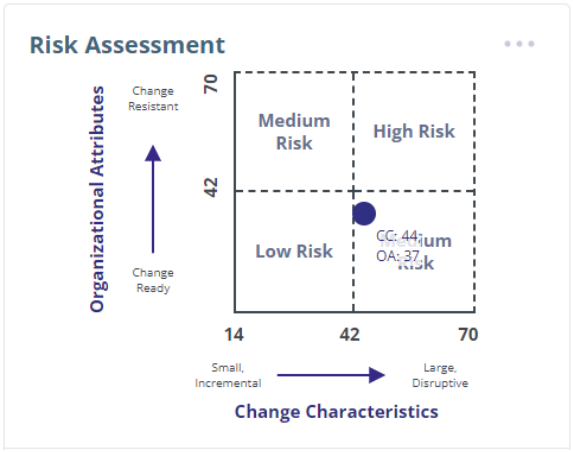
Who was involved?

From concept to fruition, various stakeholders played crucial roles in the success of the third-party risk management (TPRM) project. Legislators provided the initial funding and policy support necessary for its implementation. Agency staff from North Dakota Information Technology (NDIT), Office of Management and Budget (OMB), and Executive branch agencies were involved in the implementation phase, responsible for conducting third-party assessments and ensuring compliance with TPRM policies. Vendors participated as end-users of the assessment process, providing necessary information and undergoing security evaluations.

To secure approval, buy-in, awareness, and adoption, a comprehensive change management approach was employed, utilizing Prosci tools to ensure stakeholders had the awareness, desire, knowledge, and ability to support the project. Key communication and marketing plans were developed to inform stakeholders about the project's objectives, benefits, and requirements. Throughout the implementation,

metrics were used to measure stakeholder engagement and success, allowing for adjustments to be made based on feedback. Change management metrics were employed to guide communication efforts and ensure stakeholders remained informed and engaged throughout the project lifecycle.





Impacted Group Name	Number in Group	Y/T Status	Aspects Impacted	Degree Of Impact	Awareness	Desire	Knowledge	Ability	Reinforcement	Barrier Point
NDIT TPRM Project Staff		Completed	5	3.6	5	5	5	5	5	
OMB TPRM Project Staff		Completed	5	3.6	5	5	5	5	5	
Procurement Officers a...	150	Not Started			4	4	4	4	3	Reinforcement
NDUS	2	Not Started								
Vendors	1000	Not Started								
CSMs	10	Not Started			5	5	5	4	4	
Security GRC Team	10	Not Started			5	5	5	5	5	
State RAMP	1	Not Started								
NDIT Procurement (BB)	1	Not Started			5	5	5	5	5	

Activity Name	Impacted Group	Role(s) Required	Start Date	Finish Date	Status
Awareness					
Ongoing engagement of select vendors for Pilot. New vendors...	Vendors	Project Manager: JK - NDIT, Project Mar	Jan-01-2021	Jun-30-2023	Completed
Team communications	NDIT Procurement (BB), OMB TPRM Pr	Project Manager: TO - OMB	Jan-01-2021	Jun-30-2023	Completed
New article/reminder on TPRM	Procurement Officers and Liaisons	Project Manager: TO - OMB	May-01-2023	Jun-15-2023	Completed
New article to Procurement Officers	Procurement Officers and Liaisons	Project Manager: TO - OMB	Mar-01-2023	Mar-31-2023	Completed
Introduce TPRM project, purpose, and objectives	CSMs	Project Manager: JK - NDIT	Apr-15-2021	Apr-19-2021	Completed
Update team on need for TPRM	NDIT TPRM Project Staff	Project Manager: JK - NDIT	Dec-01-2020	Dec-01-2020	Completed
Notify StateRAMP of NDIT program/desire to join StateRAMP	State RAMP, Vendors	Project Manager: JK - NDIT, Project Mar	May-02-2022	May-02-2022	Completed
Update team on need for TPRM	Security GRC Team	Project Manager: JK - NDIT	Jan-02-2021	Jan-02-2021	Completed
Present Info at 2nd Procurement Advisory Council	NDUS, OMB TPRM Project Staff, Proc	Primary Sponsor: TO - OMB, Project Ma	Jun-13-2023	Jun-13-2023	Completed
Present Info at Procurement Advisory Council	Procurement Officers and Liaisons	Project Manager: TO - OMB	May-09-2023	May-09-2023	Completed
Email to Procurement Liaisons	Procurement Officers and Liaisons	Project Manager: TO - OMB	Dec-05-2022	Dec-05-2022	Completed
+ Add Activity					
Desire					
Ongoing engagement of select vendors for Pilot. New vendors...	Vendors	Project Manager: JK - NDIT, Project Mar	Jan-01-2021	Jun-30-2023	Completed
Team communications	NDIT Procurement (BB), OMB TPRM Pr	Project Manager: TO - OMB	Jan-01-2021	Jun-30-2023	Completed

How did you do it?

NDIT utilized ARPA funds to establish the third-party risk management program, partnering with an implementation partner to procure the necessary solution. Collaboration with the Office of Management and Budget (OMB) was essential to emphasize the importance of identifying vendor risks prior to contract signing and implementing continuous monitoring. OMB's involvement was crucial, given their administrative code governing the procurement process.

The technical architecture focused on leveraging a third-party solution to assess vendor risks, determining the level of assurance needed based on the inherent risk of the vendor. The solution streamlined the process by utilizing a questionnaire based on NIST 800-53R5 security controls, with collaboration between NDIT and OMB to ensure relevance and efficiency. Vendors with FedRAMP, StateRAMP, or HITRUST certifications were exempted from the questionnaire, enhancing the program's effectiveness and reducing administrative burden.

Impact

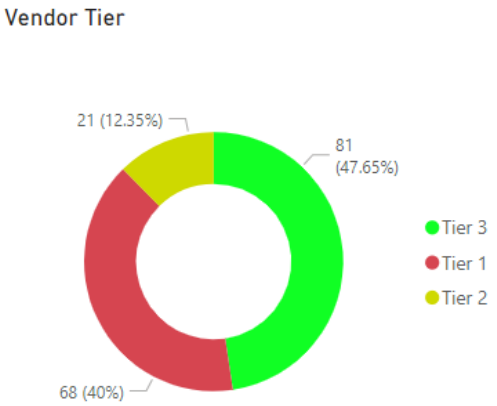
What did the project make better?

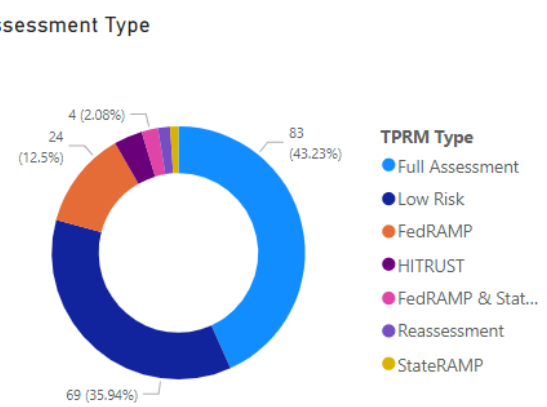
The Third-party Risk Management program significantly improved vendor assessment and monitoring processes, addressing security concerns and enhancing risk management practices. Previously, ad hoc security reviews were conducted on a limited number of vendors, lacking continuous monitoring and reassessment. With the new program, every new vendor undergoes a triage review, determining the level of due diligence required and providing visibility into all vendors and associated solutions.

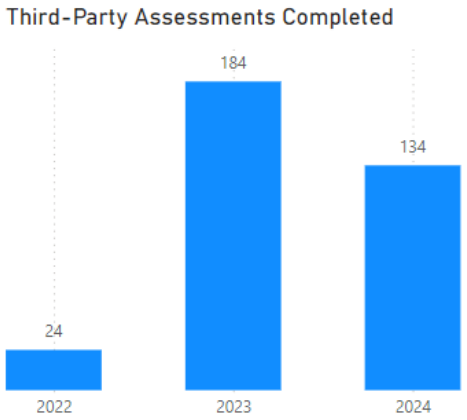
Before the project, a comprehensive vendor inventory did not exist, limiting awareness of vendors, their locations, data types, and associated risks. Today, the program has established a robust vendor inventory, enabling NDIT to identify vendors, assess their risks, and implement appropriate risk mitigation strategies. This newfound visibility has been transformative, empowering NDIT to make informed decisions and proactively manage vendor-related risks.

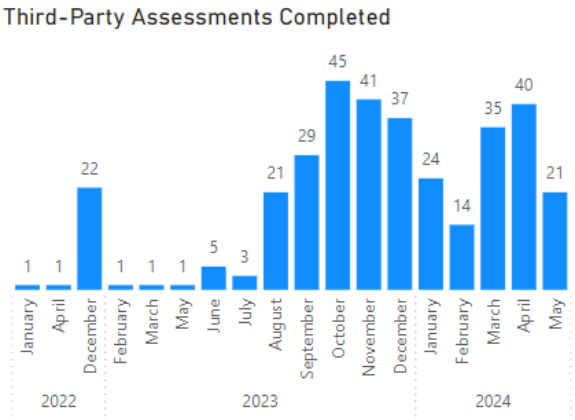
How do you know?

The TPRM program gives visibility into the type of vendors in our environment, along with the number of agencies a vendor has been assessed and the amount of vendors assessed.









What now?

Moving forward, NDIT will maintain dedicated staff and utilize the established solution for ongoing third-party risk management. Continuous funding for staff positions and the solution is essential to ensure comprehensive vendor assessments and continuous monitoring, safeguarding sensitive citizen data and upholding the state's reputation for trustworthiness.

This project warrants ongoing investment due to its critical role in protecting citizen data and maintaining trust in state services. By proactively addressing third-party risks, the state demonstrates its commitment to data security and citizen welfare, reinforcing its reputation as a reliable steward of sensitive information.

Conclusion

The implementation of ND's Third-Party Risk Management program represents a pivotal step in ensuring the security and integrity of state data in an increasingly cloud-centric environment. By adopting proactive measures to assess and monitor vendor security practices, NDIT underscores its dedication to safeguarding citizen data and maintaining public trust. As the digital landscape continues to evolve, this program stands as a beacon of innovation and resilience, exemplifying ND's unwavering commitment to excellence in cybersecurity and citizen welfare.