TEVORA™

Case Study

Demystifying Application Risks – A Detailed Case Study With Actionable Insights

Industry Context and Historical Data

To remain competitive in a fast-paced marketplace, organizations that once relied on custom-developed tools and software maintained by internal teams have shifted to a growing list of vendor-supplied applications and tools, with each vendor responsible for maintaining their security and compliance posture.

The following trends from industry-leading reports illustrate this change in further detail with context on how application-related risks are on the rise:

Large companies have an average of 211 applications within their environment. The growth of Zero Trust initiatives has also grown alongside increasing application adoption from 16% four years ago to 97% in 2022. (Okta)

Broken access controls, misconfiguration, and insufficient logging and monitoring continue to be in the top ten findings when it comes to web applications that are either vendor-supported or custom-built. (OWASP)

Many companies are over-tooling with too many applications. Over-tooling has led to an overly complicated environment with challenges in finding the talent to maintain it. Additional challenges stemming from this over-tooling include lack of visibility across services, providers, and meeting compliance requirements. (Palo Alto)

Increased reliance on a growing list of vendor-based applications mixed with custom, in-house-developed applications has proportionately increased the potential attack surface and corresponding business risk. 74% of breaches in 2022 included some human elements such as privilege misuse, use of stolen credentials, misconfiguration, or social engineering. (Verizon)

Any organization using vendor-provided applications must also maintain its risk management program to continuously assess and evaluate risks to protect the business.

Navigating Application Risks and Challenges Faced by Organizations (Identifying Potential Pitfalls and Root Causes)

Inconsistent Roles for Supply Chain & Third-Party Risk Management for Applications

Tevora has observed in its assessment of companies across industries that roles for application ownership and the corresponding management of security are often misaligned across its supply chain and third-party tools. A common risk identified in assessments involves organizations using an application to perform a business function and being responsible for configurations outside their domain expertise. These configurations include traditionally IT or security-related functions such as user provisioning and managing access control. With the growing list of web apps, cloud-based SaaS, and in-house, on-premises applications used by companies to perform essential functions, this inconsistency contributes to a significantly larger attack surface for potential threat actors.

Limited IT and Security Visibility of All Applications Within the Environment

Tevora has also observed in its assessments of organizations that comprehensive visibility of all applications within the environment (corporate and production) needs to be improved, especially with the teams often tasked with securing and configuring them. Sources of this risk include resource constraints, teams exiting without clear transition documentation, or a decentralized process for acquiring and integrating applications within the environment.

A lack of visibility into all applications used within an environment and a mismatch of roles for application ownership and management amplify the risks that could lead to a significant breach or compromise of sensitive information. From a compliance perspective, risks emerge if the assigned application owners do not understand what data is being processed, transmitted, or stored within an application. Often only after conducting an application risk assessment that an organization obtains a holistic understanding of what applications are within their environment.

How Tevora helped a global manufacturing company solve its problems (How to regain insights)

In this case study, we will describe how Tevora helped a global manufacturer conduct an enterprise-wide application risk assessment to support acquisition activities that include prioritizing remediation efforts, identifying opportunities to consolidate technology, and allocating resources to align the acquired entity's application security approach to a unified standard. To protect our client's confidentiality, we will refer to them by the fictitious Global Manufacturing Company (GMC) name.

Delivering Value for Each Audience: Executive level/business standpoint vs. technical/SME level

Executive Perspective

Tevora provided a thorough accounting of risk assessment metrics that could help answer questions about how application risks within the environment could affect the business. Deliverables included executive presentations and a comprehensive report with dashboards speaking on trends and business risks. Presentations were iterative to incorporate feedback from core stakeholders and answer these essential questions pertinent to this audience:

1	2
What are the risks related to applications from a business standpoint?	**What are the corresponding costs and investments associated with these risks to remediate or decommission them in favor of another solution?**

Financial Risks:

Analysis for financial impact to GMC was also conducted using Tevora's HydraRisk methodology which includes both qualitative and quantitative input to illustrate the impact to the business from a financial perspective. Risk assessment reporting has traditionally included updates to remediation plans and risks in more technical terms.

1	2
Excludes Business Factors	**Difficult to Calculate**

Tevora's financial impact analysis correlated with identified risks provided a clear cost and benefit for executives to make decisions. Questions answered from this analysis include:

- What will the financial impact be if we don't remediate?
- Can the business manage this risk with current resources and investments?
- Will investment in the remediation of this risk provide an advantage or reduce costs downstream?

Technical/SME Perspective

Tevora facilitated technical-level meetings with GMC's team and presented the risk register over multiple sessions to contextualize risk findings. Recommendations for industry best practice remediations correlated back to the results identified within the risk register and the control within the questionnaire. To save time and in consideration of the technical and SME perspective, the following questions were answered during the working sessions and presentations to this audience:

1	2	3
What is the expectation of SMEs when it comes to application ownership, and what is the purpose of the assessment?	**How much time will it take away from the SME to participate, and what value will they get from it?**	**What actionable insights and remediation will they get from the assessment?**

Customizing the Questionnaire to the Company's Needs:

Following discussions with all stakeholders, Tevora partnered with GMC to customize a questionnaire focused on critical application risk areas, including data and privacy classification, compliance, backups, authentication, and hardening. The questionnaire also included questions relevant to web applications and natively developed applications.

Saving Time

With tight timelines to complete this comprehensive application risk assessment, Tevora coordinated between multiple project management teams and SMEs to streamline the questionnaire facilitation and evidence collection process, with over 25 applications assessed with different teams over a few weeks.

1. *Questionnaires were provided in advance to SMEs to ensure they were prepared to answer questions and provide demonstrative evidence captured by Tevora during each interview.*
2. *Evidence collected during the interview and follow-up items were itemized and afterward organized following analysis to verify the responses given.*
3. *Interviews, even involving multiple teams and departments, averaged 30 to 60 minutes, resulting in condensed downtime for application owners and their teams.*

Tevora's initial output for immediate analysis and review was a risk register containing the following:

1. *Risk Categorization*
2. *Risk Scoring*
3. *Compliance Mapping (framework and/or policy)*
4. *Industry Recommendation for Remediation*

The register was also configured to portray glaring trends among applications for executives to analyze and for application owners to understand the gaps existing in their approach.

Contextualizing Results, identifying Risk Trends

All visuals, charts, and outcomes have been anonymized and replaced with sample data to serve as an example.

Types of applications Tevora assessed within the GMC supply chain: MFA, Finance, HR, Code Repos, Prototyping, Sales CRMs, etc.

1. ***Ranked Risks***

   As part of the risk register deliverable and final report, Tevora organized the application risks using its proprietary HydraRisk scoring model to prioritize the most critical findings to GMC. Each risk included an industry best practice remediation recommendation and detailed descriptions of the risk finding and its potential impact on the business. Additional information about the HydraRisk model can be found on the next page.

Risk Name	Application	Risk ID	Proprietary HydraRisk Model	Rating
XYZ Databases Are Unencrypted	XYZ	XYZ.2023.01		Critical
Backups Not Implemented Outside of Application	ConnectSuccess	ConnectSuccess.2023.01		High
Osulloc Server Does Not Require MFA	Osulloc	Osulloc.2023.01		High
Inconsistent Onboarding and Offboarding Access	Panam	Panam.2023.01		High
Unable to verify location of API Keys	DoubleLab	DoubleLab.2023.1		Moderate
Vulnerable Application Versions in Use	Funko	Funko.2023.01		Moderate
Lack of Password Manager	RealCoco	RealCoco.2023.01		Moderate
No User Access Logs	EverettTech	EverettTech.2023.01		Moderate
Single Application Administrator	Hakuna	Hakuna.2023.01		Moderate
Local Accounts Lacking MFA Implementation	Messer	Messer.2023.01		Moderate
No MFA Deployed for External Application Users	Hakuna	Hakuna.2023.02		Moderate
SSO Not Enabled	Funko	Funko.2023.02		Moderate
Unable to Verify Data Backup Plan	Science Web	Science Web.2023.01		Moderate
Unable to Verify Restore Capability Frequency	Science Web	Science Web.2023.02		Moderate
Ad-hoc Processes for Account User Removal	Voltorb	Voltorb.2023.03		Low
Lack of Application Enforcement Policy to Prevent Password Reuse	Funko	Funko.2023.03		Low
No Password Expiry for External Account Users	Hakuna	Hakuna.2023.03		Low

2. Financial Impact Analysis

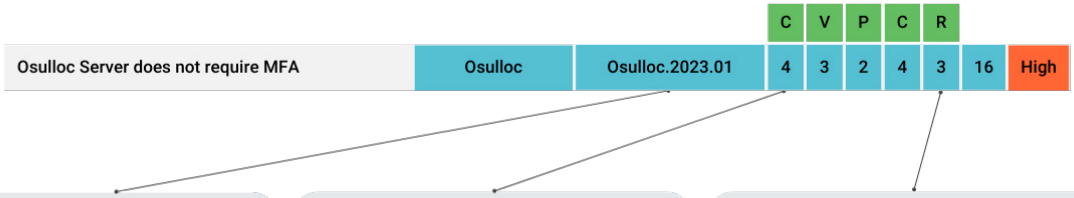
A high-level overview break down of financial impact calculation. The risk ratings considers the following criteria including but not limited to:

· Consequences (Financial impact, Strategic Risk to Goal Achievement, Reputation or Publicity, Compliance)

· Probability (Probability Percentage, Volume or Frequency, Control Implementation, Process Management Capability)

· Velocity (Complexity of Preparation, Timeframe of Occurrence)

Below are examples to illustrate how financial impact is calculated and factored into Tevora's overall application risk assessment methodology. Scoring is based on the fictitious applications and fictious risk ratings provided in this case study.



Osulloc.2023.01

Ossuloc is a critical application to GMC that contains payroll information and is a key component to GMC's HR automation workflow.

The application is relied upon through various connectors to verify sensitive personnel information and ensure payroll is processed for GMC's 3000 employees in the United States.

Applications relying on the data feeds from Ossuloc server have prevented progress in implementing MFA as it would potentially disrupt key processes to the business. Progress on this effort has been de-priotizied due to cost-saving measures and continued staffing challenges for GMC's IT and Infrastructure team.

Consequence:

If Ossuloc's server were to be compromised, the financial impact would be >$100,000 based on information gathered on how the system is used and its criticality to GMC's business goals.

- Impact to GMC's operational strategy would be impacted moderately based on the business units relying on this application.
- External exposure is high given how account access is structured, making local and/or national coverage of a breach likely and could result in reputational damage.

GMC's compliance obligations would also be impacted if breached. Regulatory violations and state-specific requirements would also be likely, though impact to overall business operations would be minimal. Remediation efforts based on the resourcing captured during this assessment would be moderate.

Assessing Financial Risk

Associated costs as part of the consequence calculation include:

- Software
- Hardware
- Outsourced operations
- Impact to operations and revenue
- Impact of record disclosure
- Impact of proprietary or protected information disclosure.

GMC should consider the scale and value of one individual's record. Current estimates for this number is approximately $165 per record. Financial risk should be evaluated based on the risk context and immediate upstream and downstream business units and solutions. Additional factors affecting the overall financial risk and consequence what ongoing costs are

- Associated with corrective actions such as cyberinsurance premiums
- Additional resourcing to demonstrate effective remediation and ongoing compliance.

			C	V	P	C	R		
No Password Expiry for External Account Users	Hakuna	Hakuna.2023.03	2	1	1	1	2	7	Low

Hakuna.2023.01

Hakuna is an RFP and bid management tool for potential contractors and vendors to submit for projects that GMC puts out for bidding.

It is managed by a small team within the procurement department and used in early stages of vetting a third-party for potential onboarding for both short and long term projects.

While there are access control mechanisms in place, configurations for external account users are less secure than what is set for internal GMC staff. This gap in configuration opens GMC up to risks around external accounts getting compromised, phishing, and privilege escalation.

Consequence:

If Hakuna were to be compromised, the financial impact would range from $75,000-$100,000 based on information gathered on how the system is used and its criticality to GMC's business goals. GMC relies upon a wide range of third parties that bid through Hakuna to execute the products and services it provides to its customers.

- Impact to GMC's operational strategy would be impacted minor based on the business units relying on this application. A breach may require suspension of its use until remediation has been completed.
- External exposure is high given how many external users are given access, though it may not be newsworthy as more critical information does not reside within the application itself

GMC's compliance obligations would also be impacted if breached in relation to contracts, agreements, and potential state-level requirements. Remediation of this risk would require minimal investment and resourcing.

Assessing Financial Risk

Associated costs as part of the consequence calculation include

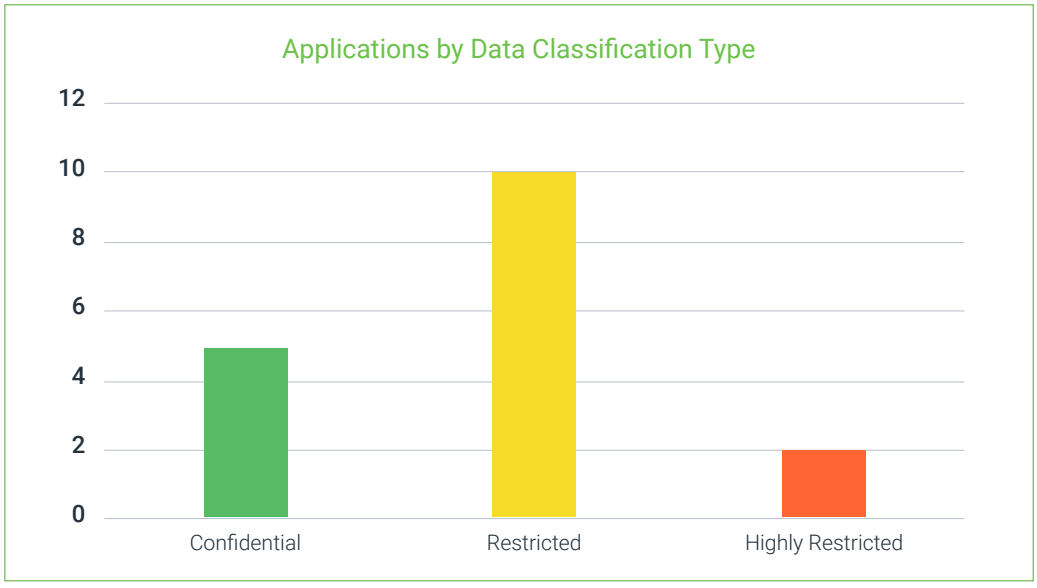
- Software
- Hardware
- Outsourced operations
- impact to operations and revenue
- Impact of record disclosure
- Impact of proprietary or protected information disclosure.

GMC should consider the scale and value of one individual's record. Current estimates for this number is approximately $165 per record. Financial risk should be evaluated based on the risk context and immediate upstream and downstream business units and solutions. Additional factors affecting the overall financial risk and consequence what ongoing costs are associated with corrective actions such as

- Cyber-insurance premiums
- Additional resourcing to demonstrate effective remediation and ongoing compliance.

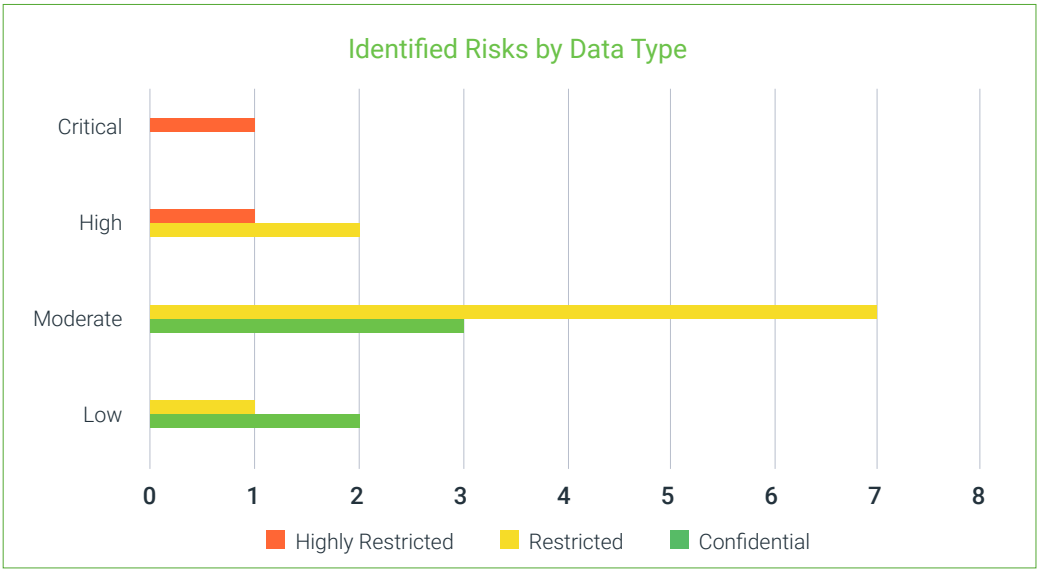
3. Overall Data Classification and Privacy Categorization Type

To ensure full transparency and visibility to all stakeholders regarding what the in-scope applications were processing, managing, and storing, applications were also organized in another view to provide high-level detail parsed out per application.



4. Risks by Data Type

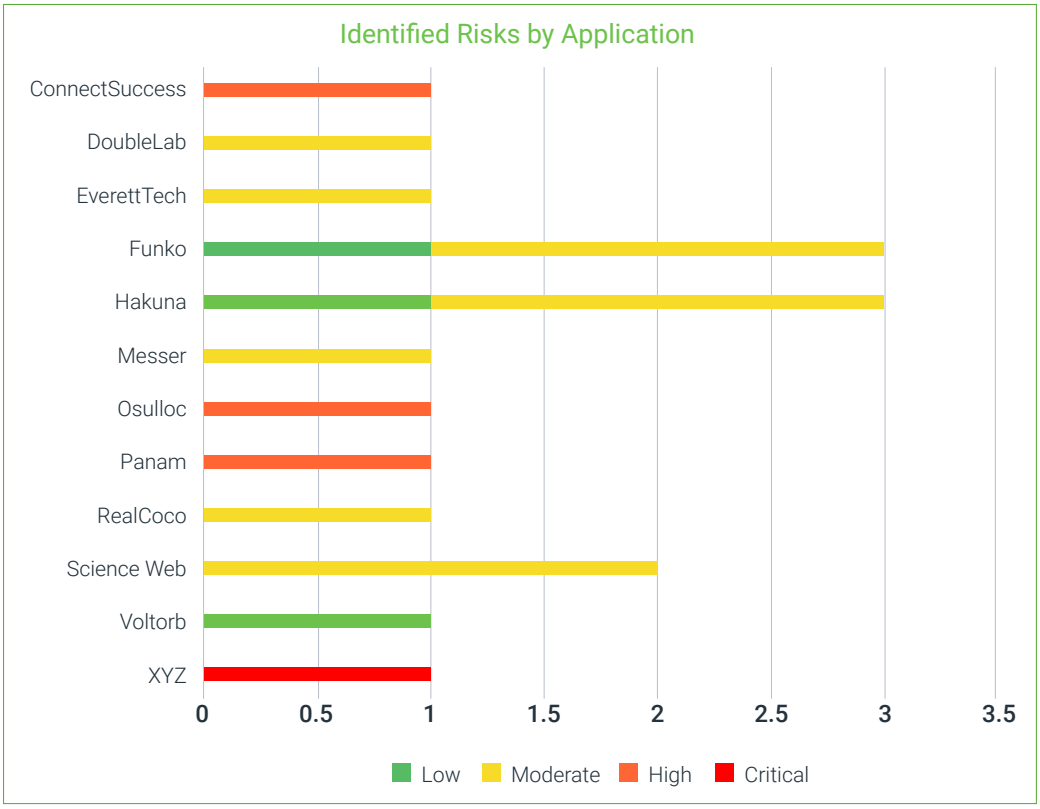
Following the overall ranking, scoring, and organizing of risks, this additional view was created to correlate the overall data classification type to the corresponding risk. As described above in Tevora's previous assessments of companies across industries, companies often do not have a comprehensive view of what data is being processed regarding compliance or regulatory definitions.



Identifying Risk Trends: data backup, access control, and compliance were among the top trends.

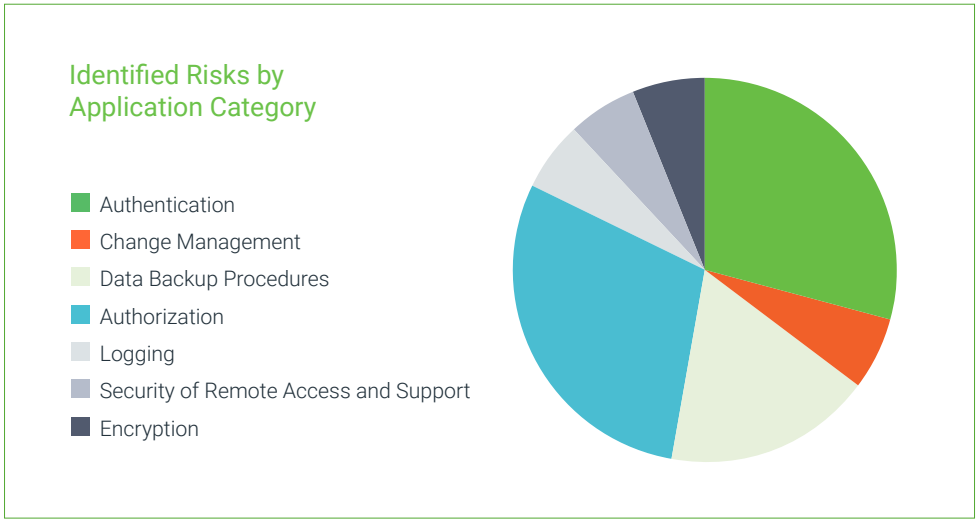
1. Risk Ratings by Application

Assessing over 25+ applications that spanned enterprise-wide, external access, and in some instances limited only to a small number of internal users. This view provided executive-level visibility into the number of risks and their criticality. One critical insight derived from this risk trend included applications onboarded during a transition of IT or security staff often resulted in department-level staff misconfiguring settings that did not adhere to the company standard.



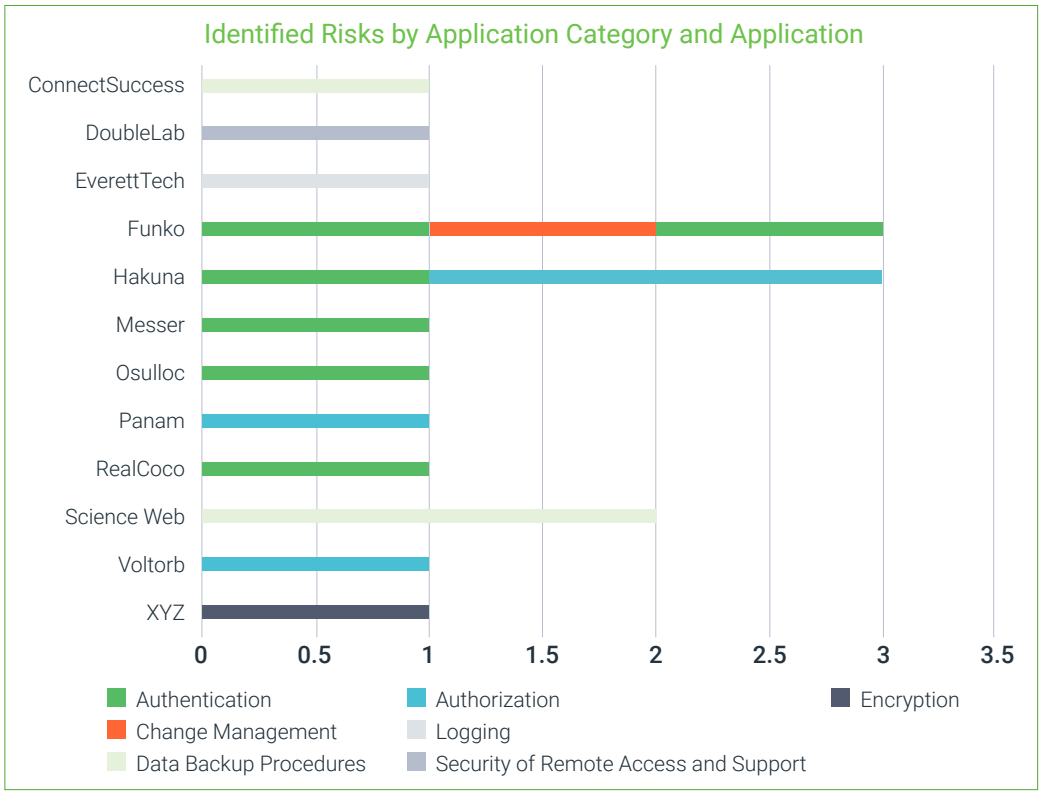
2. Application Risks by Category

From a technical and remediation perspective, this view allowed both executive and technical/SME-level stakeholders to understand the broader context of where risks fell within application categories determined from the topics covered within the questionnaire. Trends from this view included gaps in how users were managed across applications processing or storing business-critical data. Additionally, GMC had yet to conduct a thorough assessment of which applications required additional backup procedures beyond what was natively on their vendor applications.



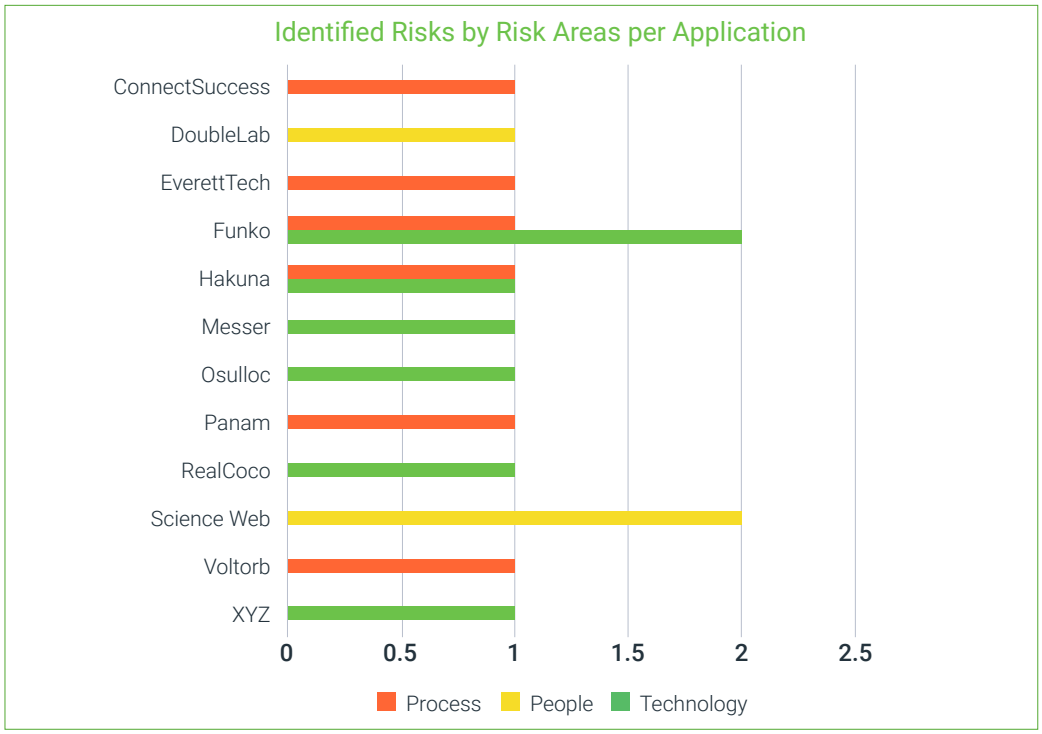
3. Application Category and Application Name

Highlighting what was working well within GMC's current application secure posture and what would benefit from additional resourcing or remediation, this view was developed. If applications did not appear on this chart, it was prefaced to GMC that those applications were meeting the agreed-upon controls determined within the questionnaire. This view also allowed technical stakeholders to map current or projected remediation plans within the respective categories to evaluate prioritization.



4. Identified Risks by Risk Area per Application:

From an executive standpoint, this view provided a detailed view by application of the general risk area that application risks fell. Operations and financial decision makers that attended presentations were appreciative that they could contextualize where resources needed to be allocated if it was determined remediation, migration, or replacement was needed for each application identified to have a risk.



Outcomes

1. Multiple applications across the enterprise did not have logs enabled or configured to forward to a central SIEM to be monitored regularly.
2. Data and privacy classification was not commonly defined or understood by application owners responsible for managing and securing them. This is a common finding among industries across application risk assessments Tevora has conducted. One example from this assessment included applications with a small user base that processed highly restricted data but did not have the corresponding security configurations to manage access.

How Tevora Can Help: Securing Deeper Visibility with Trends and Actionable Outputs

Tevora's proven and customizable approach can fit organizations of all sizes in any industry, including enterprise-level clients and small to medium-sized organizations. An established frequency of application assessments or including applications in other assessments can help organizations gain more comprehensive accountability regarding applications, homegrown, and vendor purchases. Organizations that invest significant funds in applications are ensured that each application is configured for its maximum potential, allowing organizations to gain visibility into gaps. These factors give stakeholders a clear understanding of the organization's application risk landscape, facilitating effective decision-making and proactive risk management.

Below is an example of a high-level process flow to help organizations gain visibility into their applications.

Example Process

Identification of assets, asset owners, and asset use cases throughout the organization

Identifying the asset allows Tevora to understand the applicable policy, procedure, or guidelines associated with the particular asset.

Once the identification is underway, our teams can identify threats that may apply to the organization.

Customized questionnaire

Tevora works with organizations to determine the priority, scope, and core problems to be addressed by the application risk assessment:

There is no "one-size-fits-all" solution given the differing needs of each company relative to their industry and customer segments.

Prioritizing Efficiency and Saving Time

Tevora understands the balance of prioritizing risk assessments against the day-to-day responsibilities of technical leaders and subject matter experts (SMEs). Questionnaires are prepared with enough context for a diverse audience to answer with necessary details for risk analysis, ensuring thorough effort within time constraints.

1. Prior to of each application interview, SMEs are provided the questionnaires in advance to ensure they have time to prepare, gather evidence, and answer questions before the interview.
Interview time is focused on a deeper dive and often completed within an hour or less.
2. If applications shared commonalities based on organization-wide policies or centralized technology to streamline privileged access management, this was captured during the analysis to prevent interview redundancy.
Broader, high-level trends of implementation or absence of its implementation across applications were shared in the report for technical and executive- level presentations.

Evidence Analysis

1. Tevora captures screenshots as evidence to correlate responses from SMEs and verify adherence to the controls developed for the questionnaire in conjunction with existing policies, procedures, and hardening guidelines.
2. Suppose more evidence is required in the form of screenshots captured during interviews. In that case, a detailed accounting with follow-up items is provided to the client with clear deadlines to keep the assessment on schedule.

Project Tracker and Risk Register

All information and evidence captured are documented in a Tracker with the following example details:

1. Example Categories: Application Vendor Name, Data Type, Finding Title, Category, Application Summary, Risk Category, Risk Ranking, Tevora Recommendation
2. Risk Summary Table with Risk Ranking based on Tevora's proprietary quantitative and qualitative hybrid risk model.
   a. HydraRisk Model Risk Scoring

Risk Assessment Model

Tevora worked with GMC to enhance and facilitate a questionnaire covering security controls and domains identified by the company with the corresponding acceptance criteria to determine whether each application owner and SME interviewed met the requirements. Additionally, Tevora collaborated with the client to identify additional questions and controls to provide a comprehensive view of the environmental risks.

- Common factors considered: sensitivity of the data, the type of data being processed by the application, what measures are taken to secure the application, etc.
- Areas of focus for this assessment included access controls, cryptography, data and privacy classification, and best practices around redundancy that included backups and restore capability, among many others.

In addition to the client's requirements and questionnaire, Tevora applied the HydraRisk model to score and rank the identified risks resulting from the assessment. Tevora can utilize an established internal risk scoring model or align identified risks with our HydraRisk Model.

The **HydraRisk Model** is a proprietary quantitative and qualitative hybrid risk model developed by Tevora. While it draws from NIST 800-30 and NIST CSF, many aspects of the model are based on lessons learned from Tevora's extensive work with clients to help them implement risk models. Tevora's model merges the best components of all other models to help organizations effectively assess strategic and security risks. HydraRisk accomplishes this without requiring deep statistical resources and requirements. However, it does provide more quantitative metrics than a purely qualitative model. These quantitative metrics give the organization strong justification for expenses required to mitigate identified risks.
The four steps of the HydraRisk risk management process are summarized below.

For more details on the **HydraRisk Model,** check out this blog post.