TIR-20260603 How Small Security Gaps Turn into Major Security Incidents

6/3/2026

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

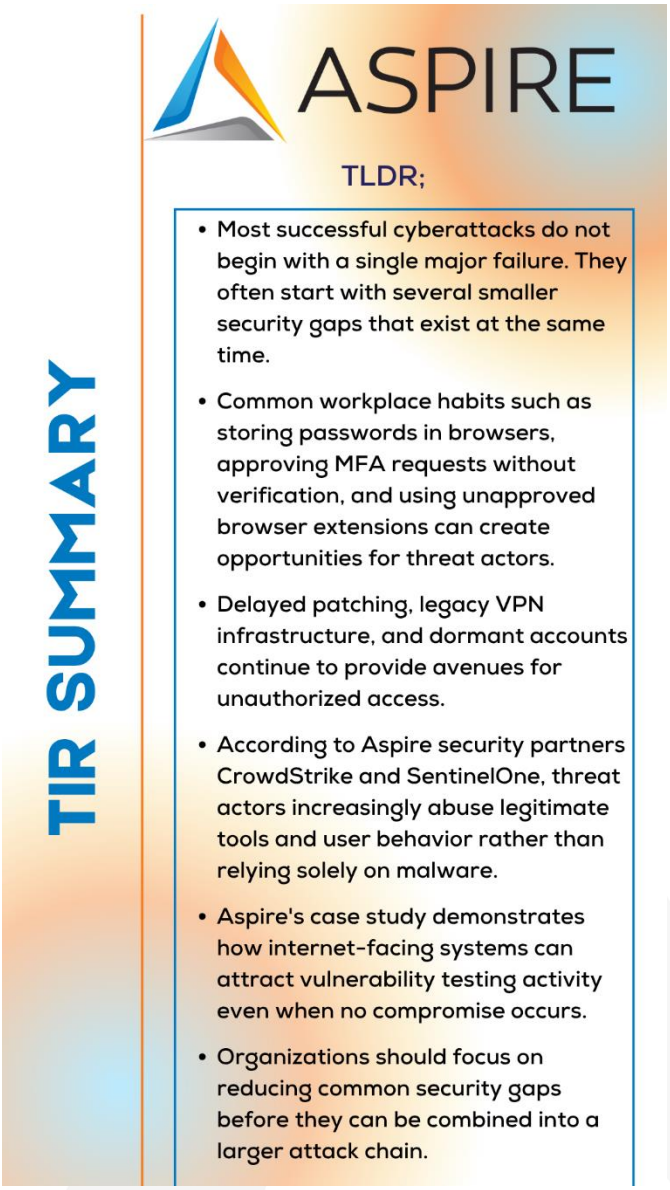
Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

Executive Summary

When people think about a cyberattack, they often picture malware or some sophisticated exploit. In reality, many incidents start with something much smaller. A password saved in a browser, an old account that was never removed, a missed software update, or an employee approving an MFA request without realizing it was fraudulent can give a threat actor the opening they need. On their own, these issues may not seem urgent. Combined, they can create a path into an organization's network and business systems.



The way people work has changed. Employees check email from their phones, log into cloud applications from home, and collaborate through platforms such as Microsoft Teams, OneDrive, and SharePoint throughout the day. These tools help organizations stay connected and productive, but they also create more opportunities for attackers. Instead of trying to break through security controls, attackers often look for ways to take advantage of legitimate access and routine workplace activity that already exists inside an organization.

Security today looks very different than it did a decade ago. Employees work remotely, use cloud apps across devices, and rely on collaboration platforms every day. That flexibility boosts productivity, but it also creates more openings for attackers. Small security gaps can quickly turn into major incidents.

WORKPLACE BECOMES AN ATTACK SURFACE

Employees Work Remotely

Work looks different than it did a few years ago. Employees work remotely and spend much of their day on cloud applications. Many use their phones for MFA or check email away from their desks. These changes make work easier, but they also create more opportunities for threat actors.

Threat actors pay attention to routine workplace activity. A compromised account often attracts less attention than malware. Remote access systems remain a common target because employees rely on them every day. Normal business activity can provide the cover needed to move through an environment without raising immediate concern.

Key Points:

- Remote workers frequently access company resources from unmanaged networks.
- Security teams have less visibility into activity occurring outside corporate environments.
- Cloud applications and SaaS platforms create additional exposure points.
- Compromised remote access credentials can provide direct access to business systems.

Employees Move Between Personal and Work Devices

Many employees use a personal cell phone to approve an MFA request so they can log into an application on their work computer. It happens all day, every day. Employees also check work email from their phones, access cloud applications outside the office, and switch between personal and company devices depending on where they are working. According to one survey, [1]43% of remote workers use personal devices instead of company-issued equipment.

Most people do not think twice about doing this because it has become part of normal work. The challenge is that personal devices are not always monitored or managed the same way as company-owned systems. An employee may receive several MFA

[1] *Lookout.com*

requests throughout the day and approve them without much thought. A login from a personal device may not attract attention because it looks like routine activity. Those everyday actions can make it easier for suspicious activity to blend in with legitimate work.

Key Points:

- Personal devices often lack the monitoring and security controls present on managed systems.
- Employees frequently move between personal and business accounts.
- Lost or stolen devices may expose business applications and authentication tools.
- Threat actors increasingly target identities rather than devices because identities travel between systems.

Convenience and Fatigue Creates Opportunity for Attackers

Employees are focused on getting their work done, not thinking like a cybercriminal. A password gets saved because it's convenient. An MFA request gets approved because it looks routine. The same habits that make work easier can also make security teams' jobs more difficult.

Saved Browser Passwords

The problem is that browser-stored credentials have become a common target for infostealer malware. Infostealers are designed to collect usernames, passwords, session cookies, and other data stored in web browsers. In many cases, that information is later sold or shared with other threat actors on the dark web. A compromised browser can provide access to cloud applications, webmail, VPN portals, and internal business systems without requiring the attacker to exploit a vulnerability.

AI Tools and Browser Extensions

AI tools have become common in many workplaces. Employees use them to help write emails, summarize information, answer questions, or complete tasks more quickly. In

many cases, employees start using these tools before IT or security teams know they exist. A browser extension gets installed, an account is connected to Microsoft 365, or company information is entered into a chatbot without much thought about where that data goes next.

Security researchers refer to this as "Shadow AI." The term describes AI tools being used without approval or oversight from the organization. Most employees are not trying to bypass security controls. They simply find a tool that helps them work faster and start using it.

The concern is not the technology itself, but visibility. Some AI tools request access to company accounts as part of setup, while others retain prompts or conversation history. When organizations do not know which tools are being used, it becomes much harder to understand where business information is being stored and who can access it.

MFA Fatigue

Multi-factor authentication (MFA) remains one of the most effective security controls available. However, threat actors have developed ways to abuse it.

MFA fatigue attacks happen when an attacker repeatedly sends authentication requests to a victim after obtaining valid credentials. The goal is to overwhelm the employee until they eventually approve a request either accidentally or out of frustration. Threat groups including LAPSUS$, Scattered Spider, and others have successfully used this technique.

An employee does not need to intentionally bypass security for this attack to work. They just need to be distracted during a meeting, responding to multiple messages, or rushing between tasks.

Key Points:

- Browser-stored passwords create opportunities for credential theft.
- Unapproved AI tools may introduce security and privacy risks.
- MFA fatigue attacks exploit human behavior rather than technical weaknesses.
- Small productivity shortcuts can become security issues when combined with stolen credentials.

IT Gaps

IT teams have a lot to manage, and sometimes things fall through the cracks. A delayed patch, an aging VPN appliance, or an account that was never removed can create opportunities a threat actor may eventually find.

Delayed Patching

Not every delayed patch is the result of a technical challenge. Sometimes an IT team is juggling multiple projects, responding to help desk requests, supporting users, or dealing with higher priorities. A patch gets scheduled for next week and then slips to the following week. Before long, a known vulnerability remains exposed much longer than intended.

Threat actors count on that happening. They know organizations do not patch every system immediately, especially when resources are limited or teams are stretched thin. Once details about a vulnerability become public, attackers often begin looking for organizations that have not gotten around to applying the update.

Legacy VPN Infrastructure

VPNs remain an important part of many environments, particularly for remote workers. However, aging VPN appliances and outdated remote access infrastructure continue to be frequent targets.

A compromised VPN can provide direct access to internal resources. If a threat actor already possesses valid credentials, an outdated VPN appliance may make their job even easier. Legacy VPN infrastructure can create risk when it remains in use long after it should have been upgraded or retired. Older appliances may contain known vulnerabilities, while unused VPN accounts are sometimes left active and forgotten.

The 2021 Colonial Pipeline ransomware attack is one example. An unknown affiliate of the ransomware operation, DarkSide, gained access using credentials for an inactive VPN account that did not have multi-factor authentication enabled. The account was tied to a legacy VPN profile that was no longer being used, but it had never been removed. After gaining access, DarkSide was able to deploy ransomware, leading

Colonial Pipeline to temporarily shut down fuel operations across much of the East Coast.

Dormant Accounts

Removing accounts after an employee leaves sounds simple, but it does not always happen right away. An account may be overlooked during an offboarding process or left active because someone thinks it might be needed later. Over time, those accounts can be forgotten entirely.

Threat actors look for that kind of opportunity. An account that no one is actively using may not attract much attention if it suddenly becomes active again. If the account has elevated permissions, it can provide access to systems and data that would otherwise be harder to reach.

Key Points:

- Patch delays create opportunities for exploitation.
- Legacy VPN infrastructure expands the attack surface.
- Dormant accounts provide additional paths for attackers.
- Outdated systems often become stepping stones for deeper access.

TRUSTED BUSINESS TOOLS GET ABUSED

Threat actors do not always need malware to accomplish their goals. In many cases, they use the same tools employees use every day. According to Aspire security partner CrowdStrike, [2]82% of detections in 2025 were malware-free. Rather than relying on traditional malware, many threat actors used valid accounts, legitimate tools, and trusted services that were already present in the environment. That means activity associated with an intrusion may look very similar to normal business activity.

These tools include:

- Microsoft Teams
- SharePoint

[2] CrowdStrike.com

- OneDrive
- Slack
- Zoom
- PowerShell
- Windows Management Instrumentation (WMI)
- Remote Desktop Protocol (RDP)
- Remote management platforms

According to Aspire security partner CrowdStrike, the growth of remote work, cloud adoption, and personal device usage has dramatically expanded the number of systems and applications that organizations must defend. Threat actors increasingly target those environments because they provide more opportunities to blend into legitimate activity.

Attackers prefer trusted tools because their activity often resembles normal business operations. Downloading files from SharePoint, using PowerShell, accessing Teams/Webex, or launching a remote support application may not immediately appear suspicious. The result is that malicious activity becomes harder to distinguish from legitimate work.

Aspire Case Study

Delayed Patching

In May 2026, Aspire's Security Operations Center (SOC) investigated suspicious activity involving two internet-facing Citrix servers belonging to a customer. CrowdStrike detected a legitimate IIS web server process (w3wp.exe) making DNS requests to an external domain linked to vulnerability testing activity. The activity did not appear to result in a compromise, but Aspire’s SOC analysts investigated further to determine what triggered the requests.

During the investigation, analysts found evidence that an external IP address attempted to exploit a web application. The affected servers also contained several publicly visible vulnerabilities identified through internet-facing scanning services. While no successful exploitation was identified, the activity indicated the servers were being targeted. Aspire's SOC continued to investigate the activity and conducted additional scans of the

affected servers. The suspicious domain was blocked in Cisco Umbrella, and the customer implemented IIS URL rewrite rules to prevent similar requests. The source IP address was blocked at the firewall and logging was increased to support further monitoring. Analysts found no evidence that the threat actor gained access to either server.

What Could Have Been Done Differently

The investigation found no evidence that the threat actor gained access to either server. However, the activity showed that the organization's internet-facing systems were attracting attention.

The servers contained publicly visible vulnerabilities, and visibility into DNS activity was limited because they were not fully monitored through Cisco Umbrella. While no compromise occurred, the case shows how exposed systems can become targets for vulnerability testing and reconnaissance activity.

IT Team

- Address publicly known vulnerabilities as quickly as operationally possible.
- Review internet-facing systems regularly to identify exposed services and outdated software.
- Confirm all internet-facing assets are sending logs and DNS activity to approved monitoring tools.
- Retire or replace systems that can no longer be maintained properly.
- Periodically review externally accessible systems through tools such as Shodan to understand what information is visible to the public.

Organization

- Assign ownership for all internet-facing systems.
- Give IT teams time to address publicly disclosed vulnerabilities.
- Track remediation efforts for externally exposed assets.
- Support replacement of aging or unsupported systems.
- Require periodic reviews of internet-facing infrastructure.

What an Attack Chain Looks Like

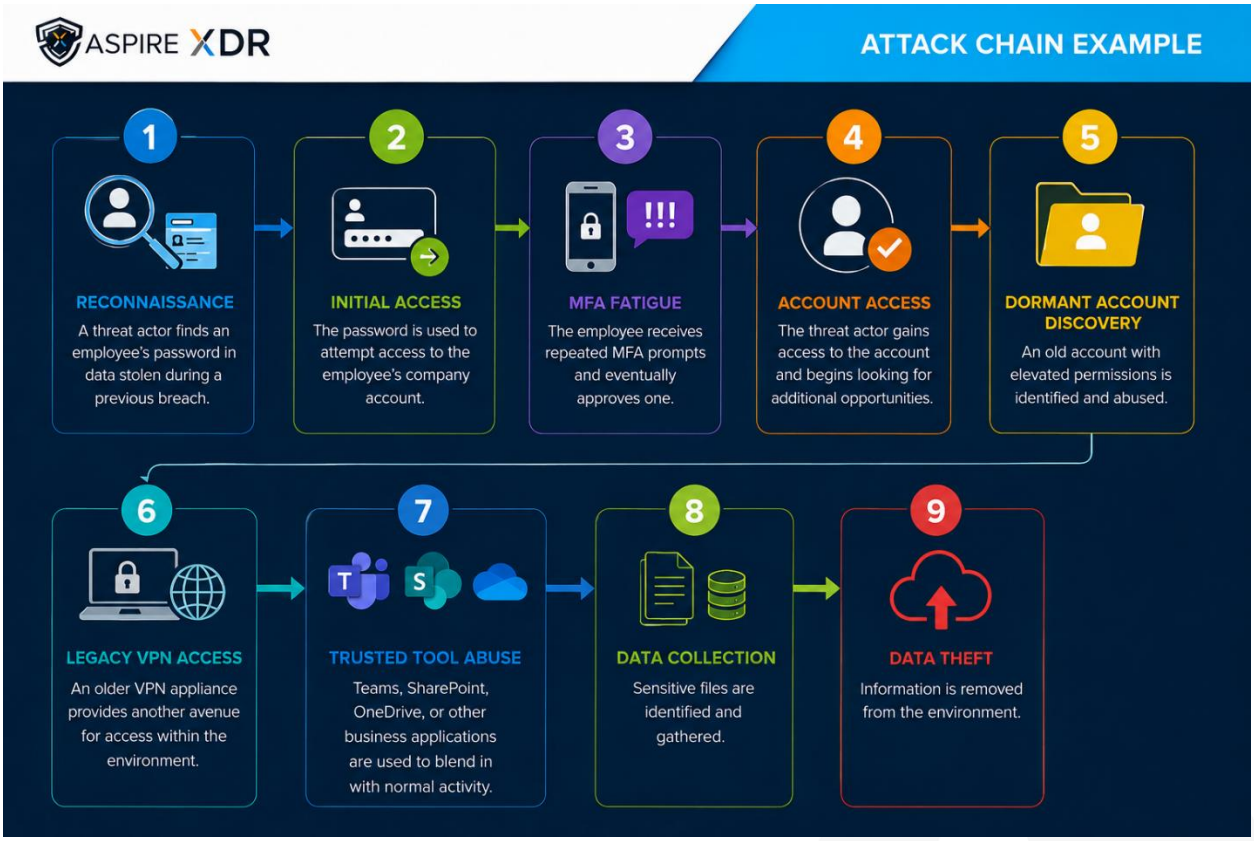
Most security incidents do not begin with a ransomware note or a major system outage. They begin with a series of smaller events that connect over time. Security teams often refer to this progression as an attack chain.

The example below shows how a threat actor could take advantage of several of the issues discussed throughout this report. No single step results in a compromise. The risk comes from how each step builds on the one before it. A realistic workplace attack chain might look like the following.

Attack Chain Example

1. Reconnaissance – A threat actor finds an employee's password in data stolen during a previous breach.
2. Initial Access – The password is used to attempt access to the employee's company account.
3. MFA Fatigue – The employee receives repeated MFA prompts and eventually approves one.
4. Account Access – The threat actor gains access to the account and begins looking for additional opportunities.
5. Dormant Account Discovery – An old account with elevated permissions is identified and abused.
6. Legacy VPN Access – An older VPN appliance provides another avenue for access within the environment.
7. Trusted Tool Abuse – Teams, SharePoint, OneDrive, or other business applications are used to blend in with normal activity.
8. Data Collection – Sensitive files are identified and gathered.
9. Data Theft – Information is removed from the environment.

Image 1: An Attack Chain



CONCLUSION

There is no single fix for every security risk. The goal is to identify the small issues that often go unnoticed and address them before they become bigger problems. In many cases, the difference between a blocked intrusion and a successful compromise comes down to whether those issues were found by the organization or by a threat actor.

RECOMMENDATIONS

Organizations should view these small security gaps as connected pieces of a larger security issue. Reducing risk requires addressing employee behavior, technical controls, and operational processes.

Workplace Becomes an Attack Surface

- Require device enrollment and security controls for devices accessing business applications.
- Review remote access logs for unusual locations, impossible travel activity, and unfamiliar devices.
- Enforce conditional access policies for cloud applications.
- Require encryption on devices used to access company resources.
- Conduct periodic reviews of BYOD policies and remote work security requirements.

Convenience and Fatigue Create Opportunity

- Disable browser password storage where practical and require approved password managers.
- Audit browser extensions and remove unapproved extensions from managed systems.
- Establish approved AI tool lists and communicate acceptable use policies.
- Train employees on MFA fatigue attacks and unexpected authentication prompts.
- Review OAuth permissions granted to third-party applications connected to Microsoft 365 and Google Workspace.

IT Gaps

- Prioritize patching of internet-facing systems and actively exploited vulnerabilities.
- Maintain an inventory of VPN appliances, remote access solutions, and exposed services.
- Conduct quarterly reviews of employee, contractor, and service accounts.
- Remove dormant accounts promptly.

- Review privileged account assignments regularly and reduce unnecessary access.

Trusted Business Tools Get Abused

- Monitor PowerShell, WMI, RDP, and remote management software usage.
- Review OneDrive, SharePoint, Teams, and cloud storage access patterns for anomalies.
- Alert on large file downloads, unusual sharing activity, and abnormal authentication events.
- Audit third-party SaaS integrations and OAuth-connected applications.
- Restrict installation rights for remote management and administrative software.

Understanding the Attack Chain

- Conduct tabletop exercises that simulate realistic attack chains.
- Map common attack paths within the environment and identify weak points.
- Monitor for credential theft indicators, MFA abuse, privilege escalation, and lateral movement.
- Use threat intelligence to understand how current threat actors gain and expand access.
- Focus on breaking attack chains early before they progress into larger incidents.

MITRE MAP

Note: These TTPs were observed by Aspire's SOC in the case study above.

Reconnaissance	T1595 – Active Scanning T1590 – Gather Victim Network Information
Initial Access	T1190 – Exploit Public-Facing Application

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.

  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.

  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

Domains

- d7qgatddbvv2uh1qucdg99bfq8tjzn5hy[.]oast[.]pro
- oast[.]pro

Process

- w3wp[.]exe (IIS Worker Process)

File Path

- \Device\HarddiskVolume5\Windows\System32\inetsrv\w3wp[.]exe

SHA-256

- a0a37fde4d8cd7385e819afa967bc525231c2f166c38591532d8feeab94e40da

Parent Process

- svchost[.]exe

User Context

- IIS APPPOOL\Citrix Delivery Services Authentication

***Note**: The domain oast[.]pro is commonly used to test whether internet-facing systems respond to specially crafted requests. Security researchers use it during vulnerability testing, but threat actors have also been observed using it to identify potentially vulnerable systems.*

SUPPORTING DOCUMENTATION

Seeing Your Attack Surface Through the Eyes of an Adversary - Palo Alto Networks

The Back Door Attackers Know About — and Most Security Teams Still Haven't Closed

When the tools you trust become the trap | The Intelligence

Multi-Factor Authentication Request Generation, Technique T1621 - Enterprise | MITRE ATT&CK®

How to Stop MFA Fatigue Attacks | Arctic Wolf

Personal Devices at Work | Nonprofit Risk Management Center

Why Remote Workforce Security Is Crucial | Scalence

What is Attack Surface Management? | CrowdStrike

Risks of Allowing Employees to Use Personal Smartphones for Business Data | ZoneAlarm Resources

The Danger of Using Personal Devices for Work And How to Make It Safe

3 Reasons Attackers Are Using Your Trusted Tools Against You (And Why You Don't See It Coming)

Commonly Abused Administrative Utilities: A Hidden Risk to Enterprise Security - Black Hills Information Security, Inc.

What Is the Cyber Kill Chain? | Microsoft Security

Colonial CEO says ransomware hackers exploited legacy VPN | Cybersecurity Dive

What is an Attack Surface? | CrowdStrike

The Impact of Remote Work on Security and Compliance

Attack Surface Risks, Challenges and Changes

What is the Cyber Kill Chain? Introduction Guide | CrowdStrike

Hackers abuse legitimate admin software to hide cyber attacks | Digital Watch Observatory

Collaboration Tools are Vulnerable: What Enterprises Need to Know - GCA | Global Cyber Alliance

Understanding the risks of AI tools: Protecting your data, devices at Ohio University

What Is Shadow AI? How It Happens and What to Do About It - Palo Alto Networks

The Hidden Dangers of Storing Passwords in Chrome or Edge — URS Cyber Resource Center

Why Storing Passwords in a Web Browser Is Risky - Information Systems & Technology

ATO Attacks from a Threat Intel Perspective | Enzoic

BYOD Security Essentials: Best Practices for Success

Seeing Your Attack Surface Through the Eyes of an Adversary - Palo Alto Networks

What Are Common Use Cases for Attack Surface Management? - Palo Alto Networks

4 Types of Attack Surface in Cybersecurity

Remote Workforce Security: Why Anti-Ransomware is Essential

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.