Metro

# Information Technology :

*Strengthen cybersecurity governance to manage risks*

June 2025
A Report by the Office of the Auditor

**Brian Evans**
*Metro Auditor*

**Maggie Muldrew**
*Senior Management Auditor*

**David Beller**
*Senior Management Auditor*

**Metro Accountability Hotline**

The Metro Accountability Hotline gives employees and citizens an avenue to report misconduct, waste or misuse of resources in any Metro or Metro Exposition Recreation Commission (MERC) facility or department.

The Hotline is administered by the Metro Auditor's Office. All reports are taken seriously and responded to in a timely manner. The auditor contracts with a hotline vendor, EthicsPoint, to provide and maintain the reporting system. Your report will serve the public interest and assist Metro in meeting high standards of public accountability.

*To make a report, choose either of the following methods:*

**Dial 888-299-5460 (toll free in the U.S. and Canada)**
**File an online report at www.metroaccountability.org**

Metro

**Brian Evans**
**Metro Auditor**
600 NE Grand Ave
Portland, OR 97232-2736
TEL 503 797 1892

MEMORANDUM

June 30, 2025

To: Lynn Peterson, Council President
Ashton Simpson, Councilor, District 1
Christine Lewis, Councilor, District 2
Gerritt Rosenthal, Councilor, District 3
Juan Carlos Gonzalez, Councilor, District 4
Mary Nolan, Councilor, District 5
Duncan Hwang, Councilor, District 6

From: Brian Evans, Metro Auditor

**Re: Audit of Information Technology**

This report covers the audit of information technology. It assessed Metro's implementation of the National Institute of Science and Technology Cybersecurity Framework. The Framework includes six functions to help organizations identify their current and desired cybersecurity levels, and areas for improvement.

We found the agency was at the initial level in several of the Framework's six functional areas. Some projects were underway to strengthen Metro's cybersecurity practices, but more work will be needed in the Govern function to prioritize investments and proactively manage risks.

We used three case studies to assess the Govern function in more depth. Risk management was a weakness across the case studies. The guidelines state that priorities and risk tolerances should be established and communicated to support operational decisions. The roles, responsibility, and authority elements were other areas that could be improved.

We have discussed our findings and recommendations with Marissa Madrigal, COO; Andrew Scott, Deputy COO; Holly Calhoun, Deputy COO; Brian Kennedy, CFO; Jeff Baer, Interim Chief Information Officer; Sam Korta, Interim Strategic Operations Director; Caleb Ford, Deputy CFO; and Adam Karol, IT Security Manager. I would like to acknowledge and thank all the people who assisted us in completing this audit.

# Summary

The Information Technology and Records Management (IT) department is responsible for managing core business systems, infrastructure, security, equipment, and user access. Over the past five years, there have been several cybersecurity incidents at Metro. Recent cyber incidents have heightened the need for business continuity planning to ensure restoration of critical services in the event of a cyberattack.

This audit assessed Metro's implementation of the National Institute of Science and Technology Cybersecurity Framework (Framework). The Framework includes six functions: Govern, Identify, Protect, Detect, Respond, and Recover. These functions help organizations identify their current and desired cybersecurity practices and areas for improvement.

We found the agency was at the initial level (*partial*) in several of the Framework's six functional areas. This meant cybersecurity risk management and governance strategies were either underdeveloped or managed in an ad hoc manner. Some projects were underway to strengthen the Identify, Protect, and Detect functions, but without more progress in the Govern function it will be difficult to prioritize investments and proactively manage risks.

Our assessment of each of the Framework functions demonstrates why Metro needs to establish goals for each. Efforts could be made to improve all six functions, but that may not align with the areas of greatest risk. To make best use of available resources, it will be important to prioritize efforts. For some Framework functions, the current level may be sufficient. This could allow Metro to focus on other needs. In other areas, like the Govern function, stronger cybersecurity practices can improve performance of the other functions.

We used three case studies to assess the Govern function in more depth. We chose case studies with varying degrees of IT and cross-department management. Two of the case studies indicated that governance was at the *risk informed* level, which meant there was awareness of risks but no organization-wide approach to managing them. The other case study was at the *partial* level, meaning limited awareness of risks and informal prioritization.

Risk management was a weakness across the three case studies. The guidelines state that priorities and risk tolerances should be established and communicated to support operational decisions. The roles, responsibility, and authority elements could also be improved.

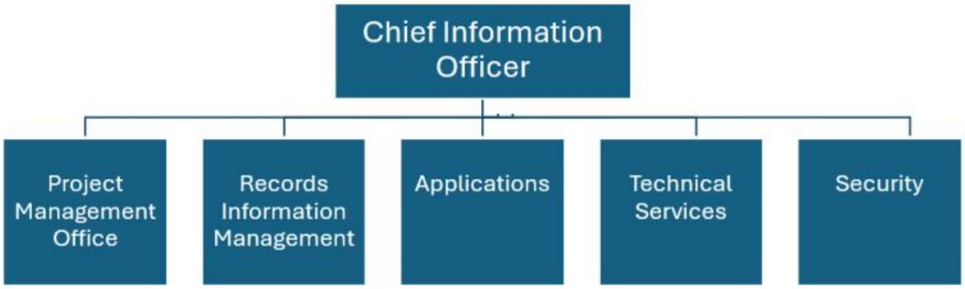
The audit includes nine recommendations. Four were designed to strengthen cybersecurity practices across the agency. Five focused on strengthening information technology governance related to timekeeping, multifactor authentication, and software purchases.

# Background

Over the past five years, there have been several cybersecurity incidents at Metro. Recent cyber incidents have heightened the need for business continuity planning to ensure restoration of critical services in the event of a cyberattack. At the same time, evolving business practices have increased flexible work environments and employees have different options for their work location, schedule, and hours. These changes increased the need for more secure remote access controls.

The Information Technology and Records Management (IT) department is responsible for managing Metro's core business systems, infrastructure, security, equipment, and user access. Inflation-adjusted expenditures rose by 13% over the last five years. Personnel services (+15%) and materials and services (+50%) experienced growth, while capital outlay fell significantly (-98%). Work is distributed across five teams. In FY 2024-25 there were thirty-nine full-time equivalent (FTE) positions across those teams.

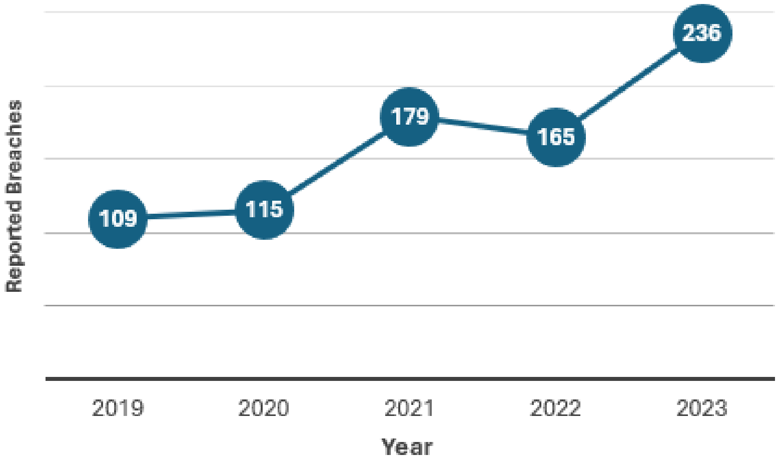
### Exhibit 1 The Information Technology and Records Management department has five teams


Chief Information Officer
Project Management Office
Records Information Management
Applications
Technical Services
Security

*Source: Auditor's Office analysis of Information Technology and Records Management organizational chart dated September 2024.*

National statistics on cyberattacks show that cyberattacks against government entities increased since 2019. Data breaches reported to the Oregon Department of Justice doubled between 2019 and 2023. Governments maintain sensitive information so protecting it against cyberattacks is a critical part of ensuring public trust.

## Exhibit 2 Reported data breaches in Oregon doubled between 2019 and 2023

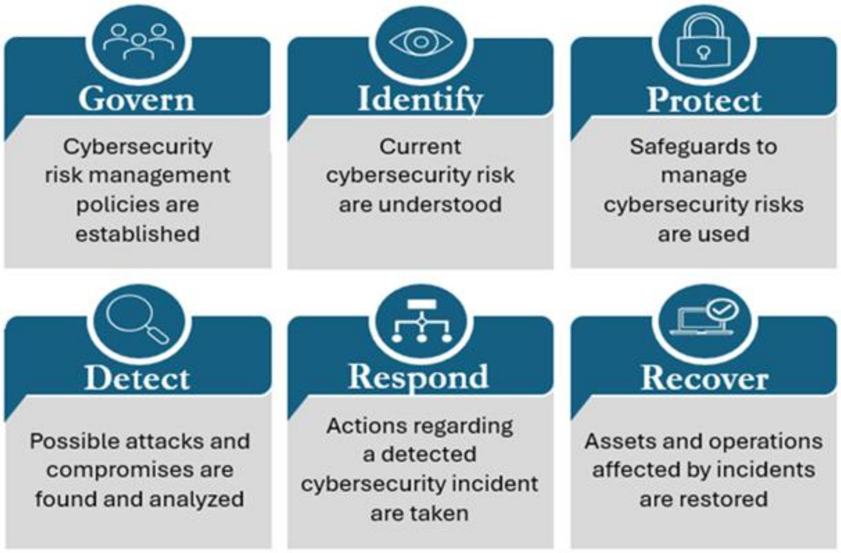


*Source: Auditor's Office analysis of Department of Justice Consumer Protection Data Breach database as retrieved on 10/29/2024.*

To manage cybersecurity risks, Metro is implementing the National Institute of Science and Technology (NIST) Cybersecurity Framework 2.0 (Framework). The Framework provides an approach to achieve cybersecurity risk management and governance objectives.

The Framework includes six functions: Govern, Identify, Protect, Detect, Respond, and Recover. These functions help organizations identify their current and desired cybersecurity practices and areas for improvement. This helps ensure cybersecurity risk management and governance aligns with organizational strategy and risks.

## Exhibit 3 The Framework addresses cybersecurity practices across six functional areas


Govern
Cybersecurity risk management policies are established
Identify
Current cybersecurity risk are understood
Protect
Safeguards to manage cybersecurity risks are used
Detect
Possible attacks and compromises are found and analyzed
Respond
Actions regarding a detected cybersecurity incident are taken
Recover
Assets and operations affected by incidents are restored

*Source: Auditor's Office illustration and summary of NIST Cybersecurity Framework v2.0 functions.*

The Framework includes a four-tier rating system to help organizations assess their level of cybersecurity practices. The lowest tier is *partial*. It describes an organization whose cybersecurity risk management and governance strategies are either underdeveloped or managed in an ad hoc manner. The highest tier is *adaptive*, and it describes organizations whose cybersecurity practices are risk-based, aligned with business strategy, formalized, communicated, and monitored.

IT's Security team is responsible for managing cybersecurity and is overseeing Framework implementation. The implementation workplan we were provided included seven steps. These steps were expected to be completed in three phases.

Phase one of the workplan was focused on projects under the Govern function, which is primarily comprised of policy development. Phase two included two parts: assessing Metro's current cybersecurity environment and setting future goals. The last phase was expected to develop action plans for specific risks and allocating resources to address them. During the audit, IT was working on the first four steps of phase one.

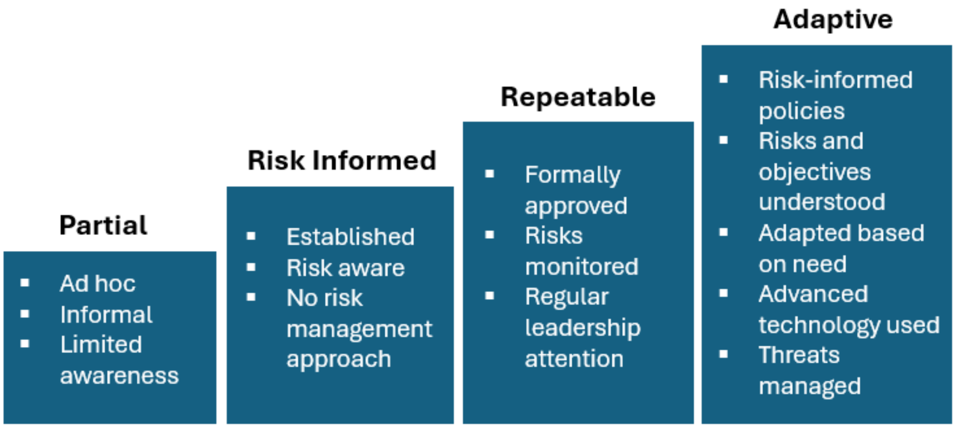
# Results

This audit assessed Metro's implementation of the National Institute of Science and Technology (NIST) Cybersecurity Framework (Framework). We found the agency was at the initial level (*partial*) in several of the Framework's six functional areas. Some projects were underway to strengthen the Identify, Protect, and Detect functions, but without more progress in the Govern function it will be difficult to prioritize investments and proactively manage risks.

This finding was similar to the conclusions reached in our 2019 audit of information technology and security. In response to increasing cybersecurity incidents since that audit, Metro identified four critical vulnerabilities that needed to be addressed to prepare for NIST implementation. One of those projects was complete and two were in progress during this audit. One had not been started.

We used three case studies to assess the Govern function in more depth. Two of the case studies indicated that governance was at the *risk informed* level, which meant there was awareness of risks but no organization-wide approach to managing them. The other case study was at the *partial* level, meaning limited awareness of risks and informal prioritization.

## Exhibit 4 The Framework includes four levels of cybersecurity practices



**Partial**

- Ad hoc
- Informal
- Limited awareness

**Risk Informed**

- Established
- Risk aware
- No risk management approach

**Repeatable**

- Formally approved
- Risks monitored
- Regular leadership attention

**Adaptive**

- Risk-informed policies
- Risks and objectives understood
- Adapted based on need
- Advanced technology used
- Threats managed

*Source: Auditor's Office summary of NIST Cybersecurity Framework v2.0 Tier components used in audit analysis*.

To improve cybersecurity practices, Metro will need to:

- Establish the level (tier) it seeks to achieve.
- Complete the risk assessment process and finalize policies.
- Prioritize resources.
- Assign roles and responsibilities.
- Address the governance weaknesses identified in three case studies.

## Metro has not set goals for cybersecurity

We found gaps indicating some cybersecurity risk management and governance practices were underdeveloped. This conclusion was based on the projects IT identified to implement the Framework and interviews. When applying principles of the Framework, organizations use tiers to describe their current and desired cybersecurity level. We were told IT was planning to establish tiers at the department level. However, this work was on hold until a risk assessment process could be developed.

Setting a goal for the desired level could help stakeholders understand what to prioritize to address weaknesses. IT has reviewed some areas of operation and identified potential improvements using the Framework. Setting expectations using the Framework's tiers could be an effective way to align available resources to the areas of greatest need.

Metro did not have a Risk Assessment policy or process. IT identified a policy for development, but it was not yet established. Under the Govern function, an organization's cybersecurity risk management strategy, expectations, and policy should be established, communicated, and monitored. Not having an established policy affected Metro's maturity under the Govern function and caused delays implementing the Framework. Accelerating the approval process for this policy is one way Metro could improve under the Govern function and advance implementation.

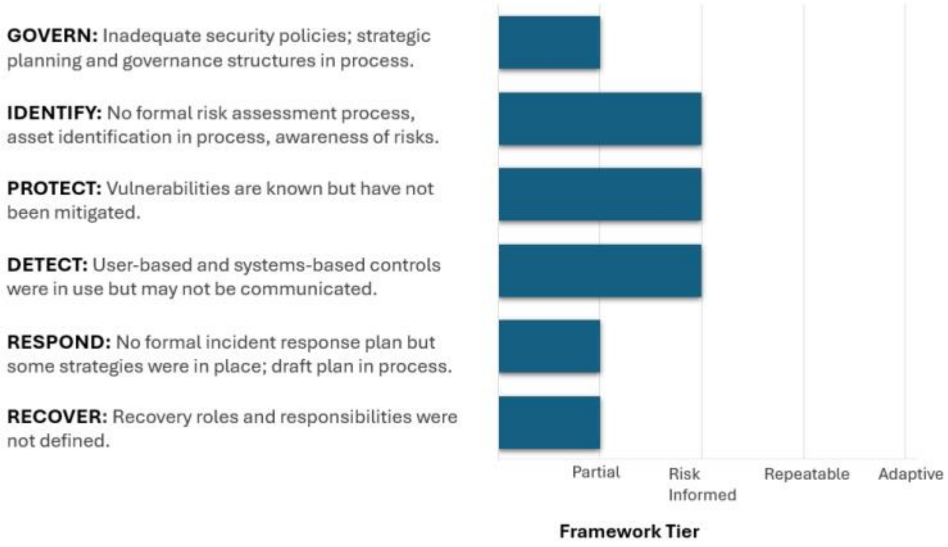
Respond
Actions regarding a detected cybersecurity incident are taken

We also found gaps in current practices under the Respond function. One example of a mature practice under this function is to execute an incident response plan once an incident occurs. We heard that an incident response plan was not in place. A draft incident response plan was provided but it was incomplete, which led us to conclude that this function was at the low end of the scale. According to the scale, a low rating is appropriate if the organization implements cybersecurity risk management on an irregular, case -by-case basis.

The Recover function focuses on an organization's ability to restore operations after a cybersecurity incident. Understanding roles and responsibilities along with executing a recovery plan were examples of mature cybersecurity practices. Staff noted that not having defined roles and responsibilities has been a longstanding issue. According to IT's implementation workplan, incident response roles were dynamic, which we interpreted to mean flexible and based on need. While adaptability is a signal of mature practices, having an established baseline for roles is expected. Since this was not the case, we estimated that practices under the Recover function were at the *partial* level.

Formally approving and communicating policies is one way to improve the Govern function. Finalizing the incident response plan and clarifying roles and responsibilities during recovery efforts could help to improve the Respond and Recover functions.

## Exhibit 5 Metro's cybersecurity practices varied between Partial and Risk Informed



*Source: Auditor's Office assessment of current practices using NIST Cybersecurity Risk Governance and Cybersecurity Risk Management tiers based on areas outlined in the implementation workplan as of January 2025and interviews.*

**Identify**
Current cybersecurity risk are understood

As reflected in the chart above, we found indications of some risk informed practices. According to the Identify function, an organization's current cybersecurity risks should be understood. Interviews with staff indicated an awareness of cybersecurity risks despite not having a formal risk assessment process. This led to a *risk informed* rating for the Identify function.

**Protect**
Safeguards to manage cybersecurity risks are used

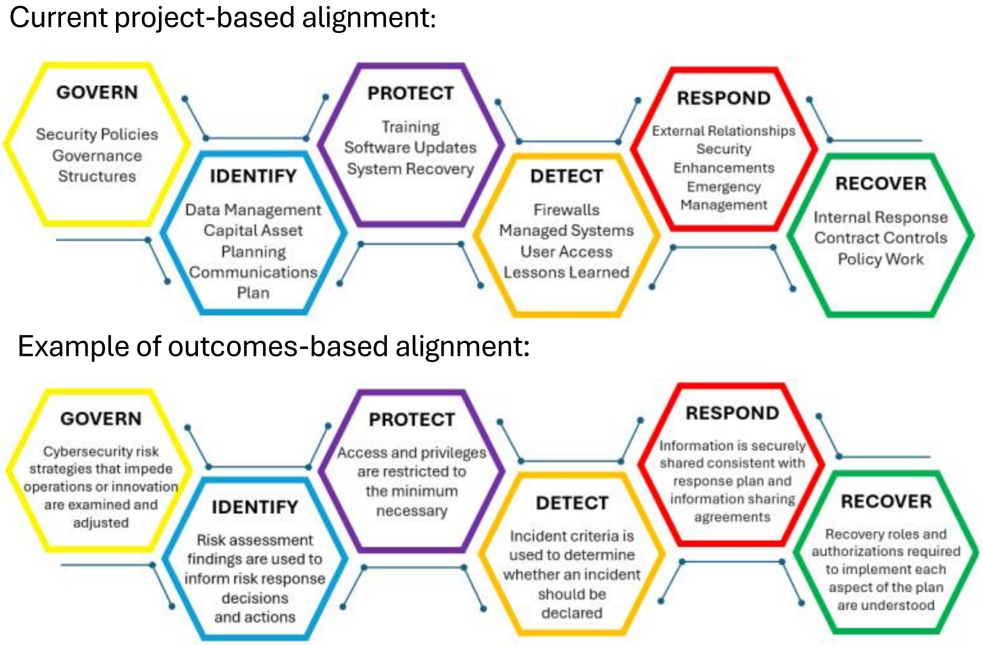
Under the Protect function, safeguards to manage the organization's cybersecurity risks are used. We heard that some risks remained unresolved despite the safeguards already in place. Some projects IT planned were aimed at addressing these risks. They use technology to help maintain the security of Metro's assets and systems functionality. They also help ensure only authorized users can access the system. Plans to incorporate improvements indicated a more *risk informed* level.

**Detect**
Possible attacks and compromises are found and analyzed

Finding and analyzing possible cybersecurity attacks and compromises are covered under the Detect function. We heard that user-based and systems-based controls were used in the detection and analysis of cyber threats. These controls were evident of a more mature, *risk informed* approach for the Detect function.

IT's workplan outlined how planned projects aligned with the Framework functions. Although projects were identified for each function, the current status and desired outcomes were not communicated. Defining outcomes is a way to prioritize and communicate the results achieved by current cybersecurity practices. Staff indicated attempts to describe current practices and compare them to the Framework were not undertaken.

## Exhibit 6 Aligning projects based on outcomes could help prioritize and communicate goals


Current project-based alignment:

GOVERN
Security Policies
Governance
Structures
IDENTIFY
Data Management
Capital Asset
Planning
Communications
Plan
PROTECT
Training
Software Updates
System Recovery
DETECT
Firewalls
Managed Systems
User Access
Lessons Learned
RESPOND
External Relationships
Security
Enhancements
Emergency
Management
RECOVER
Internal Response
Contract Controls
Policy Work

Example of outcomes-based alignment:

GOVERN
Cybersecurity risk strategies that impede operations or innovation are examined and adjusted
IDENTIFY
Risk assessment findings are used to inform risk response decisions and actions
PROTECT
Access and privileges are restricted to the minimum necessary
DETECT
Incident criteria is used to determine whether an incident should be declared
RESPOND
Information is securely shared consistent with response plan and information sharing agreements
RECOVER
Recovery roles and authorizations required to implement each aspect of the plan are understood

*Source: Auditor's Office illustration of IT project alignment to Cybersecurity Framework functions as noted in the Security Department Update (2024).*

When desired levels are not stated, it can be difficult to understand how the planned projects will affect current cybersecurity practices under each function. Knowing which outcomes have the most significant impact could help decision-makers when prioritizing investments. It can also shed light on projects that rely on other improvements to be effective. For example, investments in security policies under the Govern function alone may not be sufficient if it is not partnered with investments in training under the Protect function.

Our assessment of each of the Framework functions demonstrates why Metro needs to establish goals for each. Efforts could be made to improve all six functions, but that may not align with the areas of greatest risk. To make best use of available resources, it will be important to prioritize efforts. For some Framework functions, the current level may be sufficient, which could allow Metro to focus on other needs. In other areas, like the Govern function, strengthening cybersecurity practices can improve performance of the other functions.

## Assess organizational risks to improve the Govern Function

An effective risk assessment process is a critical part of the Govern function. It can impact the strength of the other aspects of the Framework. The purpose of a risk assessment is to evaluate current practices in relation to desired outcomes. The goal is to determine the likelihood of a cyber event and its potential impact to business functions.

An organization's approach to risks can vary. If the likelihood of occurrence and impact to business operations are considered low, an organization may choose to accept the risk and not change practices. In contrast, if either rates higher, an organization may determine that changes to mitigate or lessen risks are needed.

We were told that IT was planning to develop a risk assessment process but was hesitant to implement an agency-wide assessment without a policy to guide the process. We also heard concerns about the level of support from executive leadership and department directors. While work had begun to start the risk assessment process, it appeared to be on hold during the audit.

### Exhibit 7 The risk assessment process was on hold, which limited implementation of the Govern Function.

| Metro's Cybersecurity Projects | Started | Not Started |
|---|---|---|
| 1. Prioritize & Scope | 🟢 | |
| 2. Orient | 🟢 | |
| 3. Create Current Profile | | 🔴 |
| 4. Conduct Risk Assessment | ◑ | |
| 5. Create Target Profile | | 🔴 |
| 6. Determine, Analyze, & Prioritize Gaps | | 🔴 |
| 7. Implement Action Plan | | 🔴 |

*Source: Auditor's Office review of progress using the NIST Framework for Improving Critical Infrastructure Cybersecurity (2014) as illustrated by CISA (2023) and cited by Metro in the Security Department Update (2024).*

It was unclear how long it might take to develop a risk assessment process. Historically, IT-related policy development has not been timely. In some cases it spanned years. If that continues, progress on Metro's risk assessment could be stalled for months, if not years.

Having clarity around what the new risk assessment policy and process is supposed to achieve could help decision-makers understand its impact on improving the Govern function and implementation of the Framework as a whole. If the purpose of the risk assessment process is to evaluate existing risks to Metro's operations, then using the third-party risk assessments that have already been conducted could be useful. This could help decision-makers prioritize among the potential improvements that have already been identified.

If the goal is to assess new risks or tolerances, then identifying current practices and goals for cybersecurity could help set new baselines. Baselines can describe the current state and inform goal setting. They also help assess the significance of deficiencies to inform investments and prioritization.

## Prioritize cybersecurity efforts to align resources with risks

The audit found that resources dedicated to IT's security team were limited. Less than 10% of the department's FTE were assigned to security. During the audit, we heard that one employee spent about 15% of their time managing Framework implementation. We were told at that rate it could take two years to complete the initial implementation steps.

IT's security team is responsible for monitoring cybersecurity risks across the organization. Ensuring adequate resources are allocated in proportion to the cybersecurity risk strategy, roles, responsibilities, and policies, is one way to demonstrate mature cybersecurity practices under the Govern function.

During the audit, there appeared to be uncertainty around the level of investments needed to support cybersecurity efforts. Over the last five years, the IT department allocated less than 5% of its operating expenditures to information security. During FY 2021-22, IT moved the security function into its own work unit, but many security projects were managed across IT teams or in collaboration with other departments and venues.

Two third-party assessments of Metro's IT infrastructure and staffing levels during FY 2022-23 showed additional investments were needed. One assessment showed that Metro was spending 84% more money maintaining current capabilities, rather than transforming its business capabilities to more efficient systems. This was because most investments were tied to maintaining its data center and supporting existing software systems. It also showed that on average, Metro's percentage of total FTE allocated to IT was lower than other governments.

Since the 2022 assessments, IT spending increased by 18% and 7% in FY 2022-23 and FY 2023-24, respectively. We heard from staff that Metro was more secure today than a year ago because of these investments. While this suggests a positive trend, we also heard that underspending in IT's security team has been an ongoing issue. Although IT's total FTE increased, it remained at about 3% of the entire agency's workforce due to similar growth in the rest of the agency.

Some cybersecurity risks may remain if investments are not prioritized. We heard that the main data center needs to be relocated offsite to ensure business continuity. Some of this work was slated for FY 2024-25 and was included in IT's capital improvement plan. This indicated some prioritization was taking place. However, we also heard that similar plans had been budgeted previously but were not completed. A capital improvement project to address the data center platform was planned for FY 2022-23, but that investment did not occur as planned. This indicated that even when resources were available, improvements to advance cybersecurity were not always completed. As a result, some known risks have not been addressed.

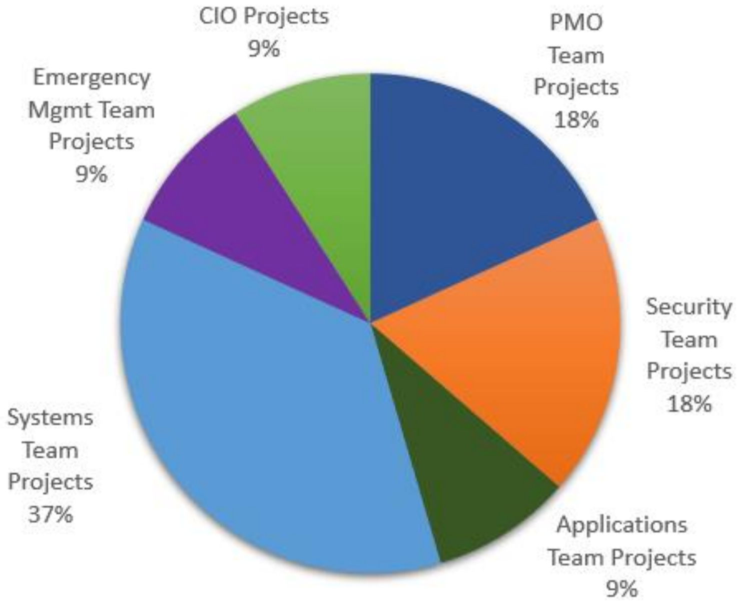
## Strengthen cross-collaboration to improve implementation

The projects in IT's Framework implementation workplan were expected to be managed by multiple teams. Two were managed by the security team and nine were either fully or partly managed by other teams. Each of the projects have the potential to impact cybersecurity outcomes in different ways so coordination and collaboration will be key to make sure these efforts have their desired effect.

The workplan we reviewed did not indicate timelines. Timing estimates were mentioned during interviews, but the basis of their determination was unclear. In one case, the suggested timelines and completion statuses conflicted. A project under the Detect function was estimated to be 60% complete and would be done by July 1, 2025. When discussing progress with the project lead, we were told progress was about 20% complete. It was expected be completed by the end of September 2025.

The workplan did not include details or descriptions of the planned projects either. To understand the scope and impact of planned projects, we had to interview employees. Similar to timelines, there were differences in the way projects were described and what they were expected to achieve. One project under the Identify function was described by one employee as including work to keep servers and systems patched. The same project was described by another employee as inventorying agency technology.

## Exhibit 8 The cybersecurity workplan was expected to be completed by a variety of different teams



*Source: Auditor's Office analysis of NIST Cybersecurity Framework projects, January 2025.*

Managing communication is important when projects involve multiple stakeholders. We heard of ongoing meetings between internal teams but it was unclear whether these teams were aware of the overall status of the workplan. One stakeholder noted their team was not kept informed of the status or goals of the improvements. The only indication of meetings or discussions centered on the Framework implementation included two quarterly briefings with executive leaders. One update occurred in October 2024. The other update was in January 2025.

If individual project leaders are not aware of how their projects align with the overall workplan, it may result in duplication of efforts and unclear deliverables. The inconsistent project descriptions and timelines provided to us indicate more clarity around expectations is needed. Documenting this information, even if brief, could help stakeholders understand each projects status and how long it will take to complete it.

During the audit, we were told IT's Enterprise Project Management Office (PMO) was in the process of creating two committees to address data management and artificial intelligence. These committees could improve the Govern function. The PMO was also managing a contract with a consultant to develop IT's strategic plan which was expected to establish a roadmap for future IT priorities.

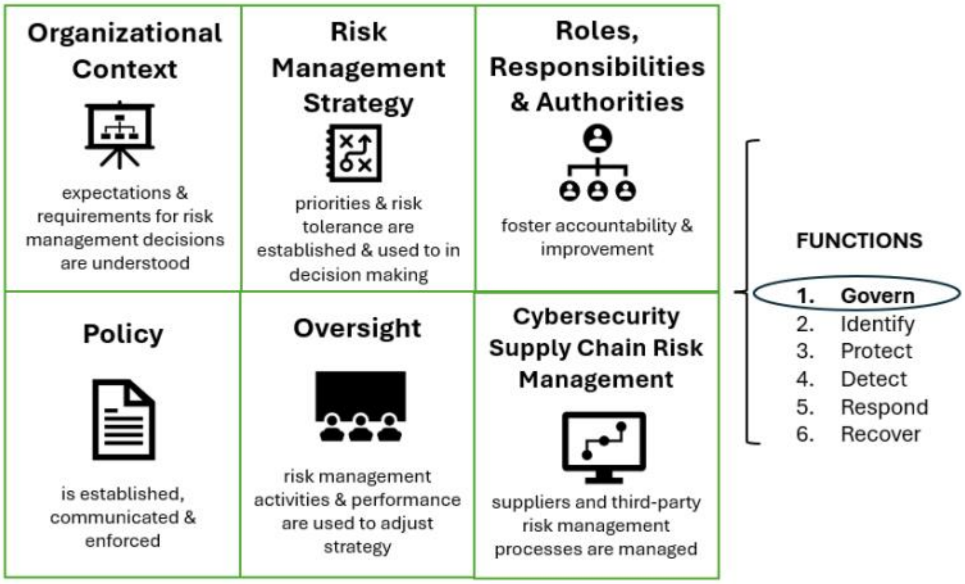
Given the breadth and complexity of the work identified in the Framework implementation workplan, it appears increased coordination with the PMO may be needed to avoid duplicative efforts among the various projects underway. One benefit could be alignment of cybersecurity objectives with IT's strategies and goals at the enterprise level. Another benefit could be more efficient use of resources among the project teams. This may add capacity to cybersecurity efforts without additional costs.

## Case studies show the need for improvements in the Govern Function

We used the Framework's guidelines for the Govern function to evaluate three case studies. The case studies provide an in depth review of the strengths and weaknesses of Metro's approach to cybersecurity. We chose case studies with varying degrees of IT and cross-department management. The case studies were:

1. Timekeeping (UKG-WFM): An agency-wide process to record employee work hours to ensure accurate paychecks.
2. Multifactor authentication (MFA): An IT-managed process to implement a security system to prevent unauthorized users from accessing employee accounts.
3. Software purchases: A jointly-managed process between IT and Finance and Regulatory Services to manage the risks associated with the purchase and installation of software.

### Exhibit 9 Case study analysis focused on NIST's Govern function


Organizational Context
expectations & requirements for risk management decisions are understood
Risk Management Strategy
priorities & risk tolerance are established & used to in decision making
Roles, Responsibilities & Authorities
foster accountability & improvement
Policy
is established, communicated & enforced
Oversight
risk management activities & performance are used to adjust strategy
Cybersecurity Supply Chain Risk Management
suppliers and third-party risk management processes are managed
FUNCTIONS
1. Govern
2. Identify
3. Protect
4. Detect
5. Respond
6. Recover

*Source: Auditor's Office analysis of NIST Framework information.*

The assessment showed that two of the case studies had governance structures at the *risk informed* level, which was higher than the average for our agency-wide assessment. This indicated these projects had established priorities and were based on identified risks. We assessed the other case study to be at the *partial* level, which indicated limited attention to risks and informal prioritization.

Risk management was a weakness across the three case studies. The guidelines state that priorities and risk tolerances should be established and communicated to support operational decisions. The roles, responsibility, and authority elements were other areas that could be improved.

## Timekeeping system governance is in place with room for improvements

We rated governance of the timekeeping system at the second level, *risk informed*. Metro uses UKG-WFM, an outside vendor for its timekeeping system. This system is important in recording employee work hours to ensure accurate pay checks. Metro's previous timekeeping system, Kronos, was discontinued in 2024. Timekeeping is a critical part of payroll processing. Payroll processing involves systems managed by IT, Finance and Regulatory Services (FRS), and Human Resources (HR). Capital Asset Management (CAM) supports continuity planning.

### Policy and oversight functions were strengths

Some strengths of timekeeping system governance were in the policy, oversight, and roles elements. Shared responsibility of Kronos management (between IT, FRS, HR) could complicate governance. However, there appeared to be strong coordination, communication, and troubleshooting between the three departments. Metro's guidance and the vendor contract define roles, responsibilities, and acceptable use for managers and employees. System downtime was used to measure performance.

Metro was able to respond to a nation-wide timekeeping outage in 2021. This appeared to be the result of a coordinated effort to utilize the timekeeping system to ensure accurate pay. During the outage, IT, FRS, HR, and other agency leaders each played roles to plan and test solutions, alter business processes to collect employee work hours, and communicate with stakeholders.

### Evolving risks require vigilance

To maintain and build on the Govern strengths we identified, a stronger risk management strategy is needed. This will likely require improvements related to roles and responsibilities and contingency planning in the event the system is down at some point in the future. While roles and responsibilities are established, recording these in a management plan would support effective operation of the system if unforeseen system disruptions or staff turnover occurs. Leaders and managers were aware of the risk of a UKG-WFM outage, but a plan to manage it was not in place. State and Federal laws require employers to pay employees accurately and on time. Any disruptions could result in negative financial effects and reduce trust among employees.

The 2021 nation-wide timekeeping outage was the result of a cyber attack. The attack caused disruptions and errors in paying workers at other organizations. Metro was able to avoid many of these issues because it had backup data that could be used to process payroll while the timekeeping system was down. Metro should be cautious that the success in 2021 does not provide a false sense of security about its ability to respond to a future outage. It was reported that the current system's features may reduce Metro's ability to use older timekeeping date in the case of an outage.

A different strategy may be needed in the case of a UKG-WFM outage. Continuing to rely on an improvised approach, rather than a predetermined plan, could delay the response to future outages. An agency-wide continuity of operations planning process is led by CAM. The continuity plan is expected to include timekeeping, but it will also include many other agency-wide operations.

Relying on the agency-wide plan appears to have tradeoffs. It appears to add capacity to get the plan finished but might slow the timeline for developing the plan related to timekeeping. Delays could increase the chance that Metro is unprepared if a timekeeping incident occurs before the plan is completed. Management stated that a payroll specific continuity plan could be created directly by FRS, but it was not complete during the audit

Disruptions to UKG-WFM have been reported recently. While one appeared to be resolved in less than one day, this suggests that future disruptions may occur. An interim contingency strategy could mitigate the risks associated with an outage until the agency-wide continuity plan is complete.

## MFA is only one part of an effective access security strategy

IT implemented a multifactor authentication (MFA) to manage access to information technology systems in FY 2022-23. This was done in response to cybersecurity insurance requirements rather than an agency-wide risk assessment. We rated MFA governance at the second level, *risk informed.*

Our assessment found elements in place for each aspect of NIST's Govern function. To maintain and improve, increased risk management strategies should be a focus. MFA was expected to help prevent unauthorized access to employees' accounts. However, the system showed some weaknesses during an August 2024 cyberattack.

## Strengths included organization, defined responsibilities, and oversight

We observed several governance strengths for MFA. MFA is used for all remote access, ensuring that users cannot use Metro's computer system without it. IT reported that employees adjusted well to the new authentication requirements. Guidance was developed and communicated to employees to ease the transition to the new system. IT plans to include policy guidance related to system access through its Framework implementation workplan.

Oversight and troubleshooting were led by an IT work group that established an oversight structure. The group monitors changes in MFA technology. Performance metrics were tracked to evaluate success. One was the number of help desk tickets related to MFA. Others included the completion rate for cybersecurity trainings and the results of internal tests to see if employees were able to identify suspicious emails. These measures indicated awareness that the success of MFA is not based entirely on technology. Employees who use the technology can strengthen its effectiveness or undermine it if they are not aware of common types of cybersecurity attacks.

## Proactive governance is needed to keep up with technology and learn from cybersecurity incidents

Although the implementation of stronger access security through MFA went smoothly, the motivations for the changes indicated an underdeveloped IT governance. Changes to insurance requirements is what motivated the change rather than an assessment of cybersecurity risk. FRS' risk management notified IT as MFA moved from a recommended practice to a requirement. Implementing MFA earlier would have signified a more advanced risk management strategy.

Similarly, the MFA system chosen was based in part on cost and the speed of implementation rather than an assessment of risk tolerances. While this appeared to result in less costs and quick implementation, it may have prevented a broader assessment of other options. For example, a different MFA configuration might have been more costly to implement initially but it might have been better able to adapt to cybersecurity risks over time.

MFA appears to be a necessary cybersecurity protection, but Metro's MFA configuration was not sufficient to prevent a cyber attack in August 2024. During the cyber attack, staff clicked on a fraudulent link and then responded incorrectly to MFA notices to verify their identity. That allowed the attacker to access employees' email accounts. Metro's experience with MFA show that security tools can be undermined when used incorrectly.

This appeared to indicate needed improvements in the areas of risk management strategy and supply chain risk management. Strengthening governance in the supply chain risk management category would include greater scrutiny around the selection and monitoring of MFA vendor weaknesses.

Metro was using an older MFA that was at the end of its lifespan. Implementing more restrictive MFA settings may be needed. IT was aware of potential weaknesses, but the vendor had not advised Metro of the specific vulnerability used in the August 2024 attack.

More collaboration between IT and FRS might have reduced some of the technological weaknesses of the MFA system. That would strengthen the *organizational context* and *roles, responsibilities, and authorities* of the Framework's Govern function. The attackers submitted a fraudulent payment request for about $500,000. The fraudulent payment request advanced for several days before it was caught.

FRS controls stopped the fraudulent payment before it was paid. However, the attack exposed weaknesses in financial controls. The connection between IT and FRS risk management practices should be coordinated to reduce that chance of fraud.

The MFA case study demonstrated the strengths and weaknesses of relying too heavily on any one security solution. Before the cyber attack, IT had purchased, but not yet implemented other security software. This suggests that IT understood its cybersecurity needs and MFA's role in them. However, the timeline for putting it into use appeared to have been slowed by limited departmental resources and capacity. An important risk management strategy is ensuring sufficient funding and staffing for these types of systems.

Clear roles and responsibilities for training was another lesson from the cyber attack. Ensuring that employees completed required training appeared to include shared roles between IT, HR, and managers within each department and venue. This structure appeared to lead to oversight weaknesses. Training records indicated that as of January 2025, 220 (17.5%) employees had not completed cybersecurity training as required. Additional steps may be needed to enforce the completion of required trainings.

## Cybersecurity requires timely implementation and clear authority to be effective

Our review of the Govern function for MFA indicated Metro may need to assign greater authority to make decisions related to cybersecurity and related system configurations. IT stated that stronger MFA configurations would require changes to business practices agency-wide. They believed more engagement from the COO's Office and Communications would be needed to effectively implement a stronger system.

For example, MFA settings can be used to limit the geographic locations allowed to access Metro's systems. We heard these types of MFA settings could be viewed as too disruptive for some employees. Other types of MFA, such as a passkey-based systems were said to present challenges for certain departments and staff.

These considerations indicate a need for Metro to establish criteria for considering tradeoffs between employee convenience and agency security. Limiting the number of devices each employee can use to authorize access appeared to be a way to improve security with limited disruption to users.

Another option would be to implement stronger MFA configurations based on an employee's level of authority at Metro. Phishing resistant MFA can function effectively with less reliance on the attention of the user. NIST recommends using phishing resistant MFAs for the most sensitive online accounts. A commitment to strong MFA governance can help Metro make the best decision about the right MFA investments based on its risk tolerance.

## Controls to limit software purchases are not aligned with current risks

Managing the software employees use is one strategy to limit cybersecurity risks. At Metro, software is supposed to be reviewed by IT before it is purchased. We rated governance of software purchases as *partial,* the first level. Policies and procedures were established but they did not appear to be functioning as expected. There were many examples of software being purchased using purchase cards, and the process to vet software purchases using the procurement process appeared to be underdeveloped.

The trend in the industry toward software as a service (SaaS) complicates governance. SaaS allows employees to purchase and use software without installing it directly on their computers. This can limit IT's awareness and ability to evaluate security needs.

Shadow IT is the term used to describe use of technology without the knowledge of the organization's IT department. Shadow IT risks include cybersecurity, compliance, data insecurity, financial waste, and operating inefficiencies. Shadow IT is common in organizations, and about one-third of cyber attacks originate from shadow IT. Free, open-source software is also a significant concern.

Metro's risk-management strategy for SaaS was underdeveloped. Clarifying what types of SasS products fit within Metro's acceptable risk tolerances would be helpful. That clarity would state in policy what SaaS products are prohibited or allowed for purchase without IT approval.

## Contracts for software purchases had more controls, but still had weaknesses

We rated software purchases made through contracts at the *risk informed* level. There was an established organizational structure with oversight roles. These elements of the Govern function depended on coordination between IT and FRS. IT was supposed to be consulted when departments wanted to contract for software. FRS oversaw the procurement process to ensure the purchases aligned with legal requirements.

Although these roles were defined, their implementation was based on a verbal agreement that FRS would inform IT about software purchase requests prior to finalizing the contract. The purpose of this arrangement was to give IT a chance to vet the software in relation to Metro's other IT systems.

In addition to informal coordination among roles, there were other processes that could reduce oversight of software purchases. Metro's Local Contract Review Board administrative rules allow software contracts to be awarded using both competitive and non-competitive processes. Non-competitive processes can have fewer checks and balances for awarding contracts.

Between FY 2017-18 and FY 2023-24 at least 77 contracts were awarded for software or other IT related products and services using the non-competitive process. This means that on average a new IT related contract was signed almost every month for the last seven years. Although we did not evaluate if these purchases aligned with special procurement rules, a contract awarded in January 2024 indicated that controls may not be working as expected. The Communications departments signed a $150k software contract without authorization from IT or FRS. Employees in Communications did not appear to be aware of contracting rules for software. After the contract was signed, IT was notified, and FRS signed a special procurement memo to justify the purchase.

The frequency of IT-related contract awards and indications that some employees were unaware of policies and rules related to software purchases suggests stronger governance was needed to manage risks. One of the reasons IT contracts are considered special procurements is it can be costly to switch providers once a system is put into use. While it can be cost-effective to have flexibility in contracting for these products and services, it makes it less likely that changes can be made in the future without significant cost. As such, strengthening governance of software purchases would help Metro manage cybersecurity, data governance, and financial risks.

We found governance of software purchases made on purchase cards (p-cards) was weak across all six NIST elements. Metro policy prohibits or restricts purchasing software on p-cards, but this was not enforced. Records showed that employees regularly purchased software on p-cards.

## Controls to limit software purchases using purchase cards were ineffective

The weaknesses we noted for software purchases appeared to be caused by weak oversight of p-card purchases generally. During the audit, we learned that timely supervisor review of p-card purchases was an ongoing challenge. In April 2025, FRS began implementing stronger controls to make sure policies were followed and accountability mechanisms were in place.

Shared responsibility among departments appeared to be one of the causes. FRS managed the p-card system and sampled transactions each month for compliance with policy. While this detective control can be helpful for addressing risks in the future, approval of the initial purchase was expected to take place within each department or work group. Each p-card holder and their manager or supervisor was expected to follow the policy and only use p-cards for approved business purposes.

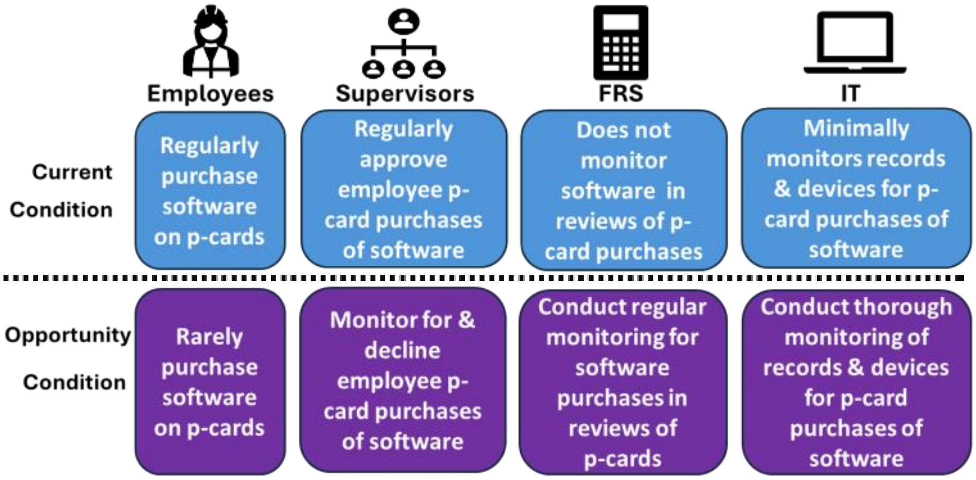
We analyzed about three years of p-card purchases from departments other than IT and excluding a videoconferencing service. About 800 purchases were made with the merchant code *Software Stores*. About 150 staff made the purchases categorized as software.

The records showed a variety of purchases that appeared to be SaaS, such as project management, cloud-based document storage, and artificial intelligence services. While all these purchases appeared to be out of compliance with the p-card policy, different types of software could present different risk profiles. For example, online file storage and project management could introduce data access, security, and redundancy risks. The risks of artificial intelligence include data security and inaccuracy.

IT provided an example that demonstrated some of the risks. A venue bought customer management software that was populated with customer data but not tied into Metro's other IT systems. The software was used by multiple employees who shared the same log-in information. IT expressed the concern that an employee who no longer worked at Metro could still log on and access customer data.

Employees who are authorized to have p-cards should be trained on acceptable use. Managers should have processes in place to verify that purchases were for an approved business purpose. FRS and IT need more consistent oversight processes to detect and correct non-compliance with policy.

**Exhibit 10 Stronger controls are needed to effectively govern software purchased on p-cards.**



|  | Employees | Supervisors | FRS | IT |
|---|---|---|---|---|
| Current Condition | Regularly purchase software on p-cards | Regularly approve employee p-card purchases of software | Does not monitor software in reviews of p-card purchases | Minimally monitors records & devices for p-card purchases of software |
| Opportunity Condition | Rarely purchase software on p-cards | Monitor for & decline employee p-card purchases of software | Conduct regular monitoring for software purchases in reviews of p-cards | Conduct thorough monitoring of records & devices for p-card purchases of software |

*Source: Auditor's Office analysis of Metro's purchase card policy, purchase card records from 9/2021 to 11/2024 and interviews.*

P-card holders may not always know what products or services are software. Software was not defined in the p-card policy, although some specific products were included in a list of prohibited products. The widespread availability of SaaS products could make it more difficult for non-IT employees to recognize these purchases as software.

The p-card data we reviewed showed a variety of accounting interpretations related to software purchases. Of the nearly 800 purchases that were assigned the merchant code, *Software Stores* by Metro's p-card vendor, fewer than 150 were classified as software purchases in Metro's accounting system. This may mean that the purchase was made from a software vendor, but it was not software. Alternatively, it may mean that software purchases were miscoded in the accounting system.

## Revising the policy and increasing training would strengthen governance

P-card records also showed that p-card holders' departments regularly coded or described purchases as software. This suggests that they often thought they were purchasing software, which would likely be a violation of the p-card policy unless they had special permission from IT. For example, in our analysis, around 600 purchases were labeled by departments with the Metro account code for software or described as software.

The frequency of software purchased on p-cards showed more oversight and training was needed to effectively manage cybersecurity risks. P-card holders may not understand the policy and there may be too many options to avoid compliance. Oversight mechanisms to detect, correct, and prevent these purchases can be strengthened and refined. IT may also need to assess if some low-risk software products should be allowed to be purchased on p-cards.

# Recommendations

To strengthen cybersecurity practices, the Deputy Chief Operating Officer or designee, Chief Information Officer, and Security Manager should:

1. Clarify roles, responsibilities, and timelines for NIST Cybersecurity Framework implementation.
2. Develop a risk assessment process to inform implementation.
3. Establish cybersecurity goals for each function.
4. Allocate resources to align recommendation two and recommendation three.

To strengthen information technology governance related to timekeeping, multifactor authentication, and software purchases:

5. IT and FRS should create a plan for responding to a timekeeping system outage.
6. IT should implement an MFA system aligned with recommendation three.
7. IT and department and venue management should ensure staff complete annual cybersecurity trainings.
8. FRS should update the purchase card policy and procedures to define what software purchases require IT approval.
9. FRS should create written guidance for roles and responsibilities related to procurement of software contracts.

## Scope and methodology

The purpose of the audit was to determine Metro's preparedness to manage cybersecurity and information technology governance risks. The scope of the audit was Metro's current practices, implementation of National Institute of Science and Technology (NIST) Cybersecurity Framework (Framework), and selected IT governance case studies over the past five years. The audit included two objectives:

1. Determine IT's readiness to implement principles of NIST Framework to manage cybersecurity risks, and
2. Determine the effectiveness of IT governance for managing risks in three case studies.

To familiarize ourselves with the audit topic, we reviewed prior audits, status of recommendations, NIST publications, publications regarding cybersecurity and information technology governance. We interviewed Metro leaders and reviewed documentation to understand current risks and carryover risks from the prior audit. Additionally, we reviewed operating and capital improvement project expenditures using data from PeopleSoft Finance for fiscal years 2019-2024. We also reviewed actual spending based on documentation from the Finance and Regulatory Services department staff for the same fiscal periods.

To address our first objective, we analyzed existing implementation documents and conducted interviews with staff. We used principles from the Framework to create a testing methodology for estimating Metro's tier level. Testing principles were developed using the six Framework functions. The levels were based on the Framework Tiers. A judgmental sample of components from each Tier of the Framework's Cybersecurity Risk Governance and Cybersecurity Risk Management tables were selected to define each level. Sample components were selected based on their applicability to the principle under review and compared against financial, documentary, and testimonial evidence. Then, using the levels, we assessed the extent to which Metro's implementation addresses the principles of the Framework.

The assessment was of limited scope and derived from implementation documents and interviews. It was not intended to represent an exhaustive assessment of Metro's enterprise-wide cybersecurity.

The second objective was to determine the effectiveness of IT governance for managing risks in three case studies. We developed a testing sheet and methodology based on the Framework governance standards. We included the six governance categories (Organizational Context; Risk Management Strategy; Roles, Responsibilities, and Authorities; Policy; Oversight; and Cybersecurity Supply Chain Risk Management).

We evaluated whether governance best practices were used in three case studies. The case studies were multifactor authentication, software purchasing, and timekeeping system (Kronos & UKG-WFM). To complete this objective, we gathered documentation and interviewed knowledgeable staff to assess the level of alignment with the Framework governance standards. We obtained purchase card data for approximately three recent years to conduct analysis of software purchases. We assessed the difference between Metro's practices and best practices and estimated the impacts of missing elements. Finally, we determined strengths, weakness, and opportunities for improved governance in each case study.

To evaluate the current status of IT governance, we assessed what risks were present from the uncompleted 2019 audit recommendations. The improvements needed to correct the Framework gaps identified were proposed. We concluded on the priorities needed to increase alignment with the different aspect of best practices.

In January 2025 we sent a separate letter to management about Metro's surveillance camera policies. Inconsistent language in some policies increased the risk of noncompliance with the records retention schedule. The letter also identified other control weaknesses related to surveillance camera use. In response, management summarized plans to address the risks identified in the letter.

This audit was included in the FY 2024-25 audit schedule. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Management response

Memo

Metro
600 NE Grand Ave.
Portland, OR 97232-2736

Date: June 25, 2025

To: Brian Evans, Metro Auditor

From: Andrew Scott, Acting Chief Operating Officer

Subject: Management Response – Information Technology Audit June 2025

Management would like to thank the Metro Auditor for reviewing our overall cybersecurity efforts and governance structure and highlighting several areas where we can continue to make improvements. Cybersecurity is an ever-evolving field, especially with threat actors becoming increasingly more sophisticated in their attacks.

Because public trust is at the heart of Metro's core values, we will continue focusing on strategic investments aimed at securing our systems and protecting our data and information from these threats. Ensuring the safety of the information held by Metro is of critical importance.

Overall, management agrees with the nine recommendations, and you will find our responses to each of these as follows:

**Recommendation 1:** *Clarify roles, responsibilities, and timelines for NIST Cybersecurity Framework implementation.*

Management agrees with this recommendation. Metro is taking steps to align its cybersecurity efforts with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 and is developing a structured approach to guide implementation. As part of this effort, we are defining key roles and responsibilities, clarifying governance structures, and identifying initial implementation priorities. This initial planning phase will help lay the groundwork for broader framework adoption and integration across the organization. We expect to complete this phase in Q4 of calendar year 2026.

**Recommendation 2:** *Develop a risk assessment process to inform implementation.*

Management agrees with this recommendation. We will develop a risk-based assessment process to inform our approach to implementing CSF 2.0. As part of this, we plan to conduct an organization-wide cybersecurity risk assessment to better understand current capabilities, resource needs, and areas of exposure. The results will guide prioritization, resource alignment, and future planning milestones. The work is expected to coincide with Recommendation 1 and be completed in Q4 of calendar year 2026.

**Recommendation 3:** *Establish cybersecurity goals for each function.*

Management agrees with this recommendation. Building on the foundational work described in recommendations 1 and 2, we will define cybersecurity objectives aligned with each function of CSF 2.0. This includes identifying appropriate target implementation tiers that reflect our risk profile and operational environment. These goals will guide the development of a cybersecurity roadmap to support phased implementation. Because this work will be informed by the results of the organization-wide risk assessment (recommendation 2), we expect to complete this effort in Q4 of calendar year 2027.

**Recommendation 4:** *Allocate resources to align recommendation two and recommendation three.*

Management agrees with this recommendation and will identify the necessary resources to implement recommendations two and three. This will include assessing staffing, funding, systems requirements, and capital project needs. As planning progresses, this work may inform budget considerations for FYs 2026 and 2027, as well as future years depending on prioritization and scope. In the short-term, the FY 2026 Budget was amended to include additional one-time resources to support this work. Management is not including a completion date for this item since it will be ongoing.

**Recommendation 5:** *IT and FRS should create a plan for responding to a timekeeping system outage.*

Management agrees with this recommendation. We will work with our timekeeping system vendor to explore service level expectations and different options to establish backups or guaranteed uptime with the intent to reduce or mitigate our risk level for this priority solution. We expect to have this completed in Q2 of calendar year 2026.

Finance and Regulatory Services (FRS) is participating in an agency-wide effort to document our continuity of operations plans (COOP) and this effort has already identified and prioritized payroll, including timekeeping, as the area where any disruption would have the highest impact. This area of the FRS COOP is targeted to be completed by the end of calendar year 2025 and will include responses to timekeeping system outages as well as other identified risks.

**Recommendation 6:** *IT should implement an MFA system aligned with recommendation three.*

Management agrees with this recommendation. We will conduct an assessment of our current Multi-Factor Authentication (MFA) environment against the goals that are established in recommendation three. We expect to have this completed soon after the cybersecurity goals are established, no later than the end of calendar year 2027.

**Recommendation 7:** *IT department and venue management should ensure staff complete annual cybersecurity trainings.*

Management agrees with this recommendation. Metro currently provides annual cybersecurity training to employees and recognizes its importance in maintaining a strong cybersecurity posture. We acknowledge the auditor's observation regarding inconsistent training completion and will work to clarify roles and responsibilities for ensuring staff compliance. As part of this effort, we will review current training procedures and tracking methods to strengthen accountability and completion rates across all departments and venues.

We note that, at the time of the audit, staff were still within the current training cycle, with completion due by June 2025. Nonetheless, we will continue to reinforce expectations across departments and clarify roles to ensure consistent tracking and accountability for future training cycles.

**Recommendation 8:** *FRS should update the procurement card policy and procedures to define what software purchases require IT approval.*

Management agrees with this recommendation. The Metro Purchasing Card (P-card) policy currently requires IT approval for all computer hardware, software, and peripherals. P-card holders are accountable for purchases made on their P-card and are responsible for following policy. FRS and IT agree that procedures and documentation should be enhanced to identify potential policy violations and determine appropriate next steps. This work will be completed by the end of calendar year 2025.

**Recommendation 9:** *FRS should create written guidance for roles and responsibilities related to procurement of software contracts.*

Management agrees with this recommendation. Procurement Services has existing practices ensuring that IT is involved whenever a department request includes software. FRS will formalize this practice into written guidance and ensure appropriate reference materials are available Metro-wide. This written guidance will be completed by the end of calendar year 2025. In addition, Metro now has outside counsel on retainer to review major software contracts for security risks.

We want to thank the Auditor again for reviewing this important area and helping to emphasize how we embrace and improve cybersecurity in the agency.

Metro

Office of the Metro Auditor
600 NE Grand Avenue
Portland, Oregon 97232
503-797-1892
www.oregonmetro.gov