Information Technology: Strengthen cybersecurity governance to manage risks

Why this audit is important

National statistics show the level of cyberattacks against government entities increased in recent years. At the state level, data breaches reported to the Oregon Department of Justice, including government and non-government entities, doubled between 2019 and 2023. Governments maintain sensitive information and provide critical services so protecting systems against cyberattacks is a critical part of ensuring public trust.

The audit assessed Metro's implementation of the National Institute of Science and Technology (NIST) Cybersecurity Framework. The Framework includes six functional areas to help organizations achieve their cybersecurity risk management and governance objectives. A four-tier rating system is used to assess each function.

The NIST framework includes six functional areas

Source: NIST Cybersecurity Framework v2.0.

What we found

We found Metro was at the *partial* tier level in several of the NIST 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 functions, but without more progress in the Govern function it will be difficult to prioritize investments and proactively manage risks.

Source: Auditor's Office summary of NIST Cybersecurity Framework v2.0.

Metro has not set goals for cybersecurity. Efforts could be made to improving 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 and increase internal coordination. For some Framework functions, the current level may be sufficient. 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. 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 were other areas that could be improved.

What we recommend

The audit included 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.

Metro

Metro Auditor Brian Evans
oregonmetro.gov/auditor