
Oregon Medical Board

IT Strategic Plan Progress Report

May 2026

Executive Summary

This report covers the first year of implementation of the Oregon Medical Board's 2025-2028 IT Strategic Plan, adopted on May 29, 2025. Since adoption, the agency has identified 60 action items across five strategic goals and has completed 23 (38%) of those items. An additional five action items are currently in progress. Since this is the first progress report under the current plan, all completed items reflect work accomplished since the plan's adoption.

Notable achievements include completing the agency's transition from VPN to Zero Trust Network Access (ZTNA), upgrading all agency workstations to Windows 11, adding online complaint submission capability for the public, completing a Center for Internet Security (CIS) controls assessment, procuring a governance, risk, and compliance (GRC) system, and fulfilling several legislative compliance requirements. The highest completion rate is in the "Support Users in All Work Environments" goal (71%), reflecting strong progress in staff-facing technology improvements.

The "Modernize Core Business Suite Software" goal reflects the lowest completion rate (14%), consistent with the long-term, multi-year nature of this initiative. Three items under this goal are actively in progress, and the agency continues to apply internal development resources to advance the modernization effort.

Since plan adoption, 18 new action items have been added during quarterly reviews to respond to emerging legislative requirements and operational needs, demonstrating the plan's design as a living document. The agency's use of Jira software to track action items, introduced with this plan, provides improved visibility and accountability for all strategic activities.

Strategic Objectives

The 2025-2028 IT Strategic Plan contains five strategic goals, each supporting the agency's mission to protect the health, safety, and wellbeing of Oregon citizens:

- **Appropriately Secure Agency Information Assets:** This goal focuses on safeguarding the agency's confidential information — including criminal history and mental health records — while ensuring appropriate access. It emphasizes compliance with recognized security standards including CIS, NIST, and CJIS, staff security awareness, and business continuity planning.
- **Modernize Core Business Suite Software:** This goal addresses the modernization of the agency's aging TechMed core business system, which supports licensing, case management, and other mission-critical processes. The agency is pursuing this through internal development of system enhancements, applying best practices for software design and user-centered development.

- **Support Users in All Work Environments:** This goal ensures that staff and board members can work effectively whether in the office or remotely. It focuses on security, efficiency, reliability, and equitable access to technology regardless of work location.
- **Maintain a Reliable Infrastructure that Utilizes Current Technology:** This goal ensures the agency's technology infrastructure remains current, secure, and reliable. It includes updating hardware and software, remediating vulnerabilities, and maintaining robust document management capabilities.
- **Respond to Evolving Legislative and Enterprise Requirements and External Party Needs:** This goal addresses the need to adapt to changing requirements from the legislature, Enterprise Information Services (EIS), and other state and federal partners. It encompasses statutory implementation, enterprise-mandated technology adoptions, and active participation in statewide IT governance.

Metrics and Targets

The performance metrics for the IT Strategic Plan implementation are provided below. Counts reflect all action items currently tracked in Jira, including items added after plan adoption. As this is the first annual report under the 2025-2028 plan, the completion rates represent cumulative progress from plan adoption through the date of this report.

Strategic Goal	Actions Identified	Actions Completed	In Progress	Completion Rate
1. Appropriately Secure Agency Information Assets	10	4	0	40%
2. Modernize Core Business Suite Software	14	2	1	14%
3. Support Users in All Work Environments	7	5	1	71%
4. Maintain a Reliable Infrastructure that Utilizes Current Technology	11	4	0	36%
5. Respond to Evolving Legislative and Enterprise Requirements	18	8	3	44%
Overall Plan	60	23	5	38%

The overall completion rate of 38% is consistent with expectations for the first year of a four-year plan, particularly given the range of multi-year initiatives included. The plan targets 100% completion of action items with required deadlines and 70% completion of items with general target deadlines. The agency has met all known required deadlines to date. The highest completion rate is in the "Support Users in All Work Environments" goal, where five of seven identified actions have been completed. The "Modernize Core Business Suite Software" goal reflects a lower rate that is expected to increase as multi-year development activities reach completion.

Initiatives

Quarterly reviews of the IT Strategic Plan allow the addition of new action items and the removal of items that no longer align with business needs, demonstrating the plan's adaptability to changing requirements and priorities. Since the plan was adopted in May 2025, the following key actions have been achieved:

1. Appropriately Secure Agency Information Assets

- Delivered annual agency-wide information security training (2025), refreshing staff knowledge and increasing awareness of current security threats and best practices.
- Reviewed and documented compliance with relevant Center for Internet Security (CIS) controls, providing a current-state assessment of the agency's security posture.
- Reviewed and documented compliance with Statewide Information Security Standards, ensuring alignment with Oregon Enterprise requirements.
- Created or procured a governance, risk, and compliance (GRC) system to streamline the assessment and reporting of compliance with various security standards, improving the agency's ability to manage and demonstrate compliance.

The following items remain in progress or are targeted for completion in 2026 under this goal: updating CJIS compliance with new standards, reviewing and documenting compliance with NIST controls, delivering 2026 annual security training, and remediating findings from the CSS 2025 assessment.

2. Modernize Core Business Suite Software

- Modernized the TechMed interface, improving the usability and appearance of the agency's core business system for staff.
- Finalized user stories documenting business requirements to guide ongoing development of TechMed enhancements.

Three items are currently in progress under this goal: enabling board members to access meeting materials directly from the core business system, improving the speed of saving and loading TechMed data, and implementing a password manager. Additional items targeted for 2026 include renewal improvements, fee changes, and AI/RAG feasibility research for medical records.

3. Support Users in All Work Environments

- Replaced Bing Maps with an alternative mapping solution, maintaining a key capability used in the public licensee verification system.
- Upgraded all agency workstations to Windows 11, ensuring staff have a current, supported operating system that improves security and performance.
- Implemented Zero Trust Network Access (ZTNA) as the replacement for the agency's VPN, providing a more secure and user-friendly remote access solution.
- Investigated the viability of Mac computers for agency use, informing future hardware procurement decisions.
- Added the ability to receive complaints online, expanding access for the public to submit complaints through the agency's web portal.

The implementation of an AI chat assistant on the external website is currently in progress. The remaining item under this goal — completing PA Modernization Phase 3 work related to HB 3036 — is targeted for a future year.

4. Maintain a Reliable Infrastructure that Utilizes Current Technology

- Completed a general infrastructure upgrade, addressing aging hardware and software components to improve reliability and performance.
- Replaced the OCR (optical character recognition) service with a current solution, maintaining a critical capability used in document processing workflows.
- Hardened Linux systems to reduce vulnerabilities and improve the security of the agency's server infrastructure.
- Improved domain security and redundancy, enhancing the resilience of core network services.

Remaining work under this goal includes migration of on-premise SharePoint, replacement and decommissioning of SCCM, upgrading Windows server versions, simplifying network configuration, and preparing for a loss-of-office continuity scenario, all targeted for 2026 or later.

5. Respond to Evolving Legislative and Enterprise Requirements

- Completed EIS Tenable migration, transitioning the agency's vulnerability scanning infrastructure to the state-provided solution in compliance with Enterprise requirements.
- Implemented Criminal Conviction Determination changes required by SB 1552 (2024), Section 44, ensuring the agency's licensing processes comply with updated statute.
- Completed the CSS CIS Controls Assessment, fulfilling the state Cyber Security Services assessment requirement.
- Implemented case categorization changes in response to the Secretary of State audit findings, improving records management and compliance.
- Added the new HPSP passthrough fee capability to support the Health Professionals' Services Program.
- Participated in statewide meetings and engaged with Enterprise partners and colleagues throughout 2025, maintaining active involvement in state IT governance.
- Completed the 2026 Open Data Initiative Phase 1 deliverables, advancing the agency's data transparency commitments.
- Responded to state foreign service requirements, ensuring the agency's compliance with applicable statutory obligations.

One item is currently in progress under this goal: implementing changes for the Five-Needle Protocol under 2025 HB 2143 (Phase 1). Additional items targeted for 2026 include applying and reinstating retention policies, issuing provisional licenses for internationally trained physicians per SB 476, and completing Phase 2 of the Five-Needle Protocol, renewal setup.

Resource Allocation

Resources have been strategically allocated across the five goals to maximize mission impact while maintaining operational continuity. The IT function operates with a biennial budget of approximately \$2 million, representing about 10% of the agency's total operational budget, allocated primarily as follows: personnel (56%), core system modernization (25%), software licenses (15%), hardware and infrastructure (2%), and security and compliance (2%).

1. **Personnel:** The agency's IT team of four — three technical specialists and one manager — has continued to balance day-to-day operations with implementing strategic initiatives. The team supports approximately 42 employees, 14 board members, and over 25,000 external users. Resolving approximately 1,000 helpdesk tickets annually, the team has effectively prioritized strategic plan activities alongside routine support.
2. **Technology Investments:** Targeted investments have been made in infrastructure upgrades, and user-facing technology improvements such as the Windows 11 rollout and ZTNA implementation. The agency's approach prioritizes investments with the greatest mission impact and leverages cost-effective solutions, including open-source and state-provided services, where appropriate.
3. **Core System Modernization:** A significant portion of the budget is directed toward modernizing the TechMed core business system through internal development of system enhancements. This approach reduces dependency on costly external vendors and leverages the IT team's direct knowledge of agency business requirements.
4. **Training and Knowledge:** Resources have been allocated to annual staff information security training and ongoing documentation of procedures and technical configurations. The adoption of Jira for strategic plan tracking enhances knowledge management and provides a structured system for recording and prioritizing work.

The agency's approach to resource allocation emphasizes flexibility, allowing for adjustments as legislative mandates, Enterprise requirements, and operational needs evolve. Application of limited IT staff resources to legislative and Enterprise compliance mandates continues to require trade-offs with other strategic priorities.

Risks and Mitigation Strategies

Several risks have been identified that may impact the achievement of the strategic objectives:

1. **Resource Constraints:** The agency's small IT team must balance operational support with strategic initiatives. Legislative and Enterprise compliance mandates frequently require diversion of resources, reducing the capacity available for internally-driven strategic goals.
 - **Mitigation Strategy:** Prioritize action items based on business impact, legal requirements, and deadlines. Leverage Jira for transparent backlog management and proactive identification of items that are no longer necessary. Identify opportunities to eliminate or defer lower-priority items during quarterly reviews.
2. **Core Business Suite Modernization Complexity:** The ongoing modernization of TechMed is a multi-year undertaking that presents risks related to scope management, resource availability, and maintaining continuity of business operations during the transition.

- **Mitigation Strategy:** Continue internal development with phased delivery of improvements. Maintain rigorous user story documentation to ensure business requirements are clearly captured. Ensure no essential functionality is lost or degraded during any transition phase.
3. **Evolving Enterprise Requirements:** Changing mandates from EIS and other Enterprise partners may require reallocation of IT resources on short notice, impacting the agency's ability to complete agency-driven strategic goals.
 - **Mitigation Strategy:** Maintain active engagement with Enterprise partners through statewide meetings and regular communication to anticipate upcoming requirements. Build flexibility into implementation plans and be prepared to reprioritize action items accordingly.
 4. **Security Threats:** The evolving cybersecurity threat landscape may require rapid response, diverting resources from planned strategic activities and necessitating unplanned remediation work.
 - **Mitigation Strategy:** Maintain current security patches and controls. Continue to improve threat detection through the GRC system and participation in state security programs. Deliver annual security training to all staff. Engage with state security partners to stay informed of emerging threats.
 5. **Technological Change:** Rapid changes in technology may render some planned actions obsolete or may require earlier-than-anticipated upgrades to maintain supported, secure systems.
 - **Mitigation Strategy:** Regularly review planned action items for continued relevance during quarterly reviews. Apply the guiding principle of practical innovation — evaluate new technologies based on tangible mission benefits rather than trends and be willing to eliminate or modify action items when they no longer align with agency needs.

Next Steps

As the agency progresses into the second year of the 2025-2028 IT Strategic Plan, the focus will shift toward items targeted for 2026 completion while continuing work on in-progress initiatives. Key elements of the upcoming work include:

1. **Complete 2026-Targeted Action Items:** The agency will focus on completing the 17 action items with a 2026 target year, including CJIS compliance updates, NIST controls review, the 2026 annual security training, network configuration simplification, SharePoint migration, SCCM replacement, Windows server upgrades, implementation of ZTNA continuation tasks, and legislative compliance items.
2. **Advance In-Progress Initiatives:** The agency will continue and complete the five action items currently in progress, including the TechMed data performance improvement, the HB 2143 Five-Needle Protocol changes, online meeting materials access, and password manager implementation.
3. **Legislative Compliance:** The agency will implement required changes for the Five-Needle Protocol renewal (Phase 2), provisional licensing for internationally trained physicians per SB 476, and PA Modernization Phase 3 (HB 3036) as required by statute.

4. **Core System Modernization:** TechMed modernization development work will continue, including renewal process improvements, fee changes, and online grand renewal modernization. The agency will also conduct research into AI and Retrieval-Augmented Generation (RAG) capabilities for medical records to inform future planning.
5. **Quarterly Reviews:** The IT Governance Committee will continue quarterly reviews of the strategic plan, updating action item status in Jira, adding new items in response to emerging needs, removing items that no longer align with business needs, and adjusting priorities as required.

Conclusion

The Oregon Medical Board has made meaningful progress in implementing its 2025-2028 IT Strategic Plan in its first year, completing 23 of 60 identified action items (38%). This reflects a solid foundation across all five strategic goals, with particularly strong progress in supporting users across work environments. The agency has fulfilled all known required deadlines and delivered on several key legislative compliance requirements.

The introduction of Jira as a tracking tool with this plan has provided improved visibility into strategic activities and enabled more rigorous quarterly review processes. Since plan adoption, 18 new action items have been added, demonstrating the plan's effectiveness as a living document that adapts to the dynamic environment in which the agency operates.

The most complex and long-horizon goal — modernizing the core TechMed business system — reflects a lower completion rate consistent with its multi-year nature. The agency continues to apply internal development resources to this effort, building incrementally on a well-documented foundation of user stories and business requirements.

As the agency enters the second year of the plan, the IT team remains committed to balancing ongoing operational support with strategic advancement, managing the trade-offs imposed by Enterprise and legislative demands, and delivering secure, reliable, and customer-focused technology services in support of the Oregon Medical Board's mission to protect the health, safety, and wellbeing of Oregon citizens.