

---

# 2014 MAJOR GOALS

## Goal 3 - Optimize Infrastructure and Secure Information

---

Shared Services

IT Business Management

Security

Disaster Recovery/COOP

### 3.1 *SHARED SERVICES*

Shared services define the state's current and future model of service delivery to agency customers. During the most recent biennium the state completed its transition to PaaS (Platform as a Service) for providing IT infrastructure services, in order to reduce costs and complexity, and produce a resilient, simplified architecture. Applications development, support activities, and desktop support typically are centered in agencies in closer proximity to the business areas and their program-specific requirements.

In conjunction with agency partners, DET is now taking the next step – undertaking a project to rationalize the assets associated with multiple, separate infrastructures into enterprise services. In a rationalized environment, the overall costs to supply infrastructure are at their lowest and are managed through mature, business-driven policies and processes. The enterprise maintains a precise inventory of hardware and software, and only purchases the licenses and computers needed as new business demands emerge. Service management can be implemented broadly for enterprise-wide functions. In short, a rationalized environment will generate further efficiencies in process and architecture and drive down overall IT infrastructure costs, while at the same time providing faster and more agile IT services for business areas.

Server virtualization remains a key strategy for producing efficiencies. Through virtualization software, a physical server can be partitioned so it functions as several “virtual servers,” where multiple operating systems can be deployed and managed at once on that single physical server. This saves money by reducing the number of physical servers needed and by cutting energy consumption, because there are fewer physical servers consuming power. The state's primary data center is now 94 percent virtualized.

### 3.2 *IT BUSINESS MANAGEMENT*

DET is currently implementing IT Business Management (ITBM) – a transparent enterprise IT financial management system that enables agency customers to focus resources on growth and innovation, and helps DET and its customers advance enterprise-wide initiatives.

The ITBM solution will allow DET to modernize and refine its chargeback procedures (many of which are manual) and documentation, as well as provide customers with a more complete and understandable bill of IT, including benchmarking and forecasting information. This in turn enables agency IT organizations to collaborate with their business partners in order to make better-informed decisions regarding how, when and where to invest valuable resources. ITBM gives DET the ability to efficiently model or craft rates and provide cost-efficiency information to customers.

### **3.3** *SECURITY*

Another key characteristic of an efficient, rationalized IT infrastructure environment is that security is proactive and provides rapid and controlled responses to threats and challenges. While we already have robust systems in place, the transition to shared infrastructure services necessitated the development of an enterprise approach to security. Although agencies previously had their own security plans, for the first time, the state has an **enterprise-wide cyber security plan**.

Incorporating the results of independent security audits and feedback from multijurisdictional partners, DET completed an **enterprise security roadmap** in mid-2013. The roadmap breaks down the state's security strategy into 12 categories and approximately 100 sub-projects and tasks, along with timelines, based on business needs, risks, and opportunities. It covers a specific three-year implementation period and will be updated annually. DET established the IT Security Program to execute the 100 sub-projects, while the ITESC designed the IT Security Program to be governed by the Cyber Security Steering Committee, which ensures the policies, controls, projects, and technologies are meeting business customers' needs.

A fundamental truth of enterprise security is that security is only as strong as its weakest link, and this philosophy drives the State of Wisconsin's efforts. For example, consistent security configurations on devices can remove the most basic security vulnerabilities, and have proven to be an effective method of repelling potential intrusions. Therefore, state agencies are establishing a standard baseline security profile for state-owned endpoints (e.g., personal computers, laptops, and devices). As state government continues to centralize data resources, this baseline security profile is crucial for endpoints authorized to connect to these resources. A 12-agency working group is producing the deliverables, including inventory information, standard endpoint security requirements, a communication strategy, and a roadmap to compliance. This first phase of **endpoint hardening** will encompass nearly 30,000 devices, while follow-up projects will include another 10,000.

Closely related to endpoint hardening is **network access control (NAC)** – a method of enhancing security by restricting the availability of network resources to only those endpoint devices that comply with defined security policies. Depending on the security profile of a user's device, NAC can restrict the data and systems available to the user, as well as employ anti-threat applications such as firewalls, antivirus software and spyware-detection programs. Several agencies have implemented NAC in their departments and DET has a project underway to provide an enterprise NAC solution.

The security roadmap includes additional important initiatives to secure the enterprise. Wisconsin has utilized a homegrown, open source-based solution, in combination with a subscription service, for centralized log management – the process of collecting, correlating and analyzing computer network security information across state government. These processes are now being replaced by an even more robust **Managed Security Services (MSS) solution** – an outsourced, state-of-the-art management of enterprise security devices, systems, and processes. The MSS includes log monitoring and management, vulnerability monitoring and management, and host and network intrusion and protection.

State government recognizes that effective cyber security is as much a people challenge as it is technical. Accordingly, an enterprise **cyber security awareness training program** is in process. The program ensures state employees are well trained in fundamental cyber security concepts and practices, as well as understand the steps they can take to protect our systems. Wisconsin is also partnering in a multi-state effort to provide best-of-breed training to state IT personnel in penetration testing, digital forensics, secure Web applications, disaster recovery, network forensics and other related cyber security skill sets. Testing and certifications are included in the program.

Fundamental to the challenge of managing people is establishing their electronic identities. An **identity access management (IAM) system** facilitates the management of electronic identities, including the technologies needed to support identity management. IAM can be used to initiate, record and manage user identities and their related access permissions in a systematic and automated manner. Wisconsin's IAM strategy seeks to improve and standardize the overall security management of state IT applications by providing a foundational framework for account provisioning and access management. The enterprise will install an industry-leading IAM product suite that aligns IAM with the IT Security Program. There is, likewise, a basic efficiency aspect to this effort – an enterprise IAM solution will eliminate the need for agencies to maintain separate (and often multiple) identities for employees and the citizens they do business with.

Reporting and metrics will be the key to verifying the overall effectiveness of the security program. Are we accomplishing our objectives? Are we reducing security risks? Are we effectively blocking intrusions and viruses? Are we doing everything in our power to protect the state's information assets?

---

## ENDPOINT HARDENING

40,000

The state's endpoint hardening will encompass nearly 40,000 devices.

---

## VIRTUALIZATION

94%

The state's primary data center now utilizes 94 percent virtualized servers.

---

## SECURITY TRAINING

40,000

State employees taking security awareness training annually

---

In implementing its cyber security plan and measuring the outcomes, the state will use guidance from the Multistate Information Sharing and Analysis Center (MS-ISAC) and the National Governors Association (NGA) Governors' Homeland Security Advisors Council (GHSAC), including these essential ongoing activities:

- Count – Knowing what's connected to and running on state networks.
- Configure – Implementing key security settings to help protect state systems.
- Control – Limiting and managing those who have administrative privileges to change, bypass or override security settings.
- Patch – Regularly updating all applications, software, and operating systems.
- Repeat – Regularizing the top priorities to form a solid foundation of cyber security for the enterprise.

The infrastructure side is keeping pace, as DET recently deployed high-end performance infrastructure to support enterprise resource planning (STAR Project), business intelligence, agency databases, and IAM. Between its emphasis on efficient, shared services and enterprise security solutions, the state is adopting an adaptable IT model that can be ready for evolving business needs and the ever-changing threat landscape.

## 3.4 **DISASTER RECOVERY / COOP**

Finally, there are the risks that aren't computer-generated. All Wisconsin state government agencies with essential services have developed continuity of operations (COOP) plans based on federal guidelines in order to deal with the potentially adverse events resulting from storms, fires, crime, or other infrastructure damage.

Recognizing that COOP planning is an ongoing, everyday process and that Wisconsin needs a standard enterprise approach for continuity program methodologies, the state is currently implementing a three-year continuity cycle for operations. These efforts include plan revalidations, new continuity software solutions, business impact analysis in conjunction with the STAR Project, and formal training, testing and exercises. Meanwhile, DOA recently entered a five-year lease for a disaster-recovery data center site that provides additional geographic and infrastructure separation from the primary state data center.

### **Security**

The Enterprise Security Roadmap breaks down the state's security strategy into **12** categories and approximately **100** sub-projects and tasks.

State of Wisconsin systems protect against an average of **200,000** scans per day – many of them from external sources searching for vulnerabilities.

*Quick Facts*