

Information Technology

The Information Technology Department (IT) consists of two main components: the Uniform Accounting Network (UAN), which is documented separately, and IT, which provides the agency's core technology services.

IT's mission is to ensure that all AOS employees — whether working from the central office, a regional site, or remotely — have timely, reliable, and secure access to the systems and tools they need. In an era of increased remote work, network stability, system performance, and security are more critical than ever. IT functions as both the technical backbone of the agency and a service provider to every AOS division.

Structure and Core Functions

IT is divided into four primary operational sections: Application Development, Network Services, End-User Support, and Graphics and Records. Each section maintains essential documentation such as disaster recovery plans, network diagrams, and process manuals.

1. Application Development

This team designs, develops, and maintains internal and external applications. The work encompasses websites, reporting tools, mobile applications, and automated data processing systems. The team also manages vendor relationships for third-party systems to ensure external platforms meet agency standards.

Key internally developed applications include:

- **Timesheet Portal:** Processes biweekly time entries to the Ohio Department of Administrative Services for payroll.
- **Hinkle System:** Facilitates the filing of annual financial statements by audit clients.
- **eServices Portal:** Allows clients to pay invoices, view reports, and update profile information.
- **IPA Portal:** Provides secure access for Independent Public Accounting firms and audit staff.
- **Financial Health Reports:** Analyzes local government financial data to flag potential fiscal distress.
- **Audit Search Tool:** Public portal for retrieving completed audits.

2. Network Services

Led by three network administrators and the Deputy CIO, Network Services manages:

- Servers, firewalls, switches, and routers.
- WAN connectivity for all AOS locations.
- User account provisioning and deactivation.
- System backups and disaster recovery.
- Endpoint, email, and web security.

Redundant backups are stored at the State of Ohio Computer Center (SOCC).

3. End-User Support

This function includes the Helpdesk and regional Primary Computer Analysts (PCAs).

- **Helpdesk:** First-line technical support, available from 7:30 a.m. to 5:30 p.m., with after-hours monitoring of voicemail and email.
- **Regional PCAs:** Provide on-site assistance, distribute and configure equipment, manage IT inventory, help train new hires, and help minimize downtime during audits.

4. Graphics and Records

Handles agency branding, visual communications, and records management. This includes maintaining style consistency across publications and safeguarding archival records.

Budget and Staffing

IT is funded primarily through the General Revenue Fund (GRF), while UAN is separately funded. The operating budget for IT is about \$5.4 million.

Staffing includes 27 employees (22 classified and 5 unclassified). This staffing mix enables both centralized management of systems and localized support for field operations.

Key Responsibilities

Beyond daily maintenance, Central IT oversees:

- Procurement review for all technology purchases.
- Onboarding and offboarding IT processes.
- Operation of mission-critical applications such as TeamMate and Microsoft Dynamics GP.

- Mobile device management for agency-issued cell phones.
- Building security systems and ID badge creation.

Given the mission-critical nature of AOS's systems, even brief outages — especially of the timesheet portal or TeamMate — can cause significant disruption to audit schedules and billing.

Challenges and Risks

IT operates under a demanding set of conditions:

- **Aging infrastructure:** Core systems like the three-node server cluster and SAN are approaching end-of-life.
- **Rising security demands:** Cybersecurity threats require proactive investment in monitoring and prevention tools.
- **Staff recruitment/retention:** Public-sector pay scales make attracting and retaining highly skilled IT professionals challenging.
- **Institutional knowledge:** Many systems are homegrown, making robust documentation and knowledge transfer vital for continuity.

These challenges must be balanced against limited budgets, the growing needs of remote work, and the necessity of aligning all technology decisions with security and operational standards.

Planned Improvements and Strategic Initiatives

Central IT is actively pursuing upgrades to modernize infrastructure and improve service delivery:

- **TeamMate upgrade:** Planning begins in spring; procurement scheduled for later in the fiscal year.
- **Website redesign:** Engaging leadership to update public sites for usability, content workflows, and design consistency.
- **Disaster Recovery Plan updates:** Adding current executive contacts and testing emergency communications using Informacast.
- **Social media administration review:** Ensuring account oversight aligns with agency policies.

These initiatives aim to improve resilience, scalability, and user experience while preparing the agency for future demands.

Metrics and Governance

Central IT tracks performance metrics to assess cost-effectiveness and service quality:

- **IT cost per employee:** \$6,350 in FY 2018, compared with Gartner's \$8,807 benchmark.
- **IT staffing ratio:** 3.2 percent of total agency headcount vs. a 3.9 percent benchmark.
- **System uptime:** 99.72 percent network availability over 10 months of FY 2018.
- **Helpdesk satisfaction:** Surveys sent to 25 percent of resolved tickets; highest satisfaction ratings tracked.

The **IT Steering Committee** has representatives from each audit region and major business units and meets monthly to review priorities. All purchases are reviewed by the Deputy CIO and approved by the CIO to maintain compliance and strategic alignment.

Commercial Software Oversight

Central IT supports two primary commercial applications:

- **Microsoft Dynamics GP (GP):** Used for audit setup, project assignments, hour estimates, and client billing.
- **TeamMate:** Centralized audit documentation platform where work papers are uploaded, reviewed, and approved electronically.

Both systems are essential to audit quality, consistency, and operational efficiency.

Documentation and Accountability

To maintain transparency and operational continuity, IT keeps:

- Detailed network diagrams.
- Disaster recovery and business continuity plans.
- Project management documents.
- Inventory logs.
- Procurement history dating back to FY 2008.

This documentation is crucial for audits, decision-making, and staff transitions.

Disaster Recovery Overview

Because AOS staff are geographically dispersed, localized outages typically do not halt statewide operations. However, extended outages of centralized systems like TeamMate, payroll, or billing would have significant effects.

IT's disaster recovery plan outlines restoration priorities, communication protocols, and coordination procedures. It integrates with broader continuity plans maintained by the agency, ensuring a unified response to major disruptions — whether caused by cyber incidents, infrastructure failures, or public health emergencies.