OSIbeyond

Strategic Technology Consulting

Technology Assessments

OSIbeyond conducts biennial technology assessments as part of a proactive IT management model. The purpose of the technology assessment is to provide organizations with the current state of technology, recommendations for the future, and budget forecasting. When performed biennially this practice results in a decrease in unexpected technology expenditures as well as overall enhancement of an organization's technology solutions. The technology assessment is a comprehensive report that provides explanation of the current configuration, industry best practice, professional recommendations, and budgetary costs.

Key Areas of Evaluation:

- Network Infrastructure
    - Internet Connectivity
- Network Security
    - Firewall & IDS/IPS
    - Email Filtering
    - Antivirus
    - Data Encryption
- Network Switching
- Server Systems
- Desktops & Laptops
- Telephony & Communications
- Document Management & Collaboration
- Web Hosting & Management
- Policies & Procedures
- Staffing & Support
    - Support Levels
    - Support Procedures
    - Staff Training
- Costs & Budgeting
- Inventory & Documentation

The objective of the technology assessment is to provide your organization with a technology management roadmap. The report is intended to be an easy to understand (non-technical) report to ensure that your organization is well informed on the various aspects of technologies used within your organization.

In addition, it is intended to ensure that your organization has clear guidance on future technology initiatives, and is financially prepared for technology investments over a three-year outlook.

IT Policy & SOP Development

No matter how cutting edge the technology an organization implements, the lack of proper IT policies negates any benefits that might have been gained by the technology. This is a common shortfall in the nonprofit & association industry.

Often times the status quo and organizational politics get in the way of implementing policies that will ultimately benefit the organization. In other cases, the lack of internal expertise or resources to develop and implement such policies are reasons for an organization not having strongly defined IT processes.

OSIbeyond

As your organization's technology partner, OSIbeyond provides technical and management expertise by identifying areas that lack adequate structure and developing policies that balance the need for governance while embracing the organization's culture. Based on these factors, OSIbeyond will implement policies in collaboration with your organization's IT, HR, and management team.

In addition to the development of the above policies, OSIbeyond will work with your organization's IT, HR, and management team to develop Standard Operating Procedures.

The purpose of IT SOPs is to ensure technology functions are properly executed to adhere to the aforementioned organizational IT polices. Key IT SOPs include:

- New Employee Onboarding
- Employee Termination
- New Contractor Onboarding
- Contractor Termination
- Incident Response
- New Desktop Build
- Hardware/Software Procurement
- Business Continuity

The combination of formal policies and standard operating procedures ensures your organization's technology operations are adequately governed.

Key IT Policies:

- Acceptable Use
- Password
- Remote Access
- BYOD
- Vendor Access Management
- Backup and Disaster Recovery
- Permission Change management
- Mobile Device Management
- Compliance and Regulatory Requirements
- Auditing and Logging
- Incident Response
- Patch Management
- Physical Security
- Network Security Change Management

Security Evaluation

As technology advances so do the threats facing organizations. Security is a growing concern for nonprofits and associations. While external security threats are always a concern, it is as important to thoroughly consider internal threats within an organization.

OSIbeyond conducts holistic security evaluations to identify potential vulnerabilities, whether it is preventing malicious external attacks, or ensuring proper practices and staff training is implemented. The security evaluation report consists of the following key areas, and may be further customized for your organization.

Network Infrastructure

- Firewall (perimeter, ingress, etc.)
- WiFi (internal, guest, etc.)
- Physical Access (office/server room)
- Anti-virus/Anti-spam Protection
- Intrusion Prevention System/Intrusion Detection System

Applications & Systems

- Active Directory Configuration
- Email Access
- Remote Access
- File/Document Access
- Business Applications (finance, HR, CMS/AMS etc.)

Data

- Internal Access Controls
  - Drive/File Permissions
  - Internal Application Access
- External Systems
  - Shadow IT Practices (personal Dropbox, Google Docs, etc.)
  - External Application Access

OSIbeyond's security evaluation may be completed in conjunction with a traditional security audit or as a stand-alone project. The evaluation focuses on business policy and procedure concerns from a high level, presented in a format that can be used by HR or management to improve an organization's security posture.

Interested In Learning More?

Contact Us