Information Technologies

ABOUT US

OUR SERVICES

FY 18/19 Goals

FY 19/20 Goals

ABOUT US

Mission Statement

The Information Technologies Department is committed to provide reliable, sustainable/modern, flexible, and effective information technology infrastructure to support the business objectives of County departments.

Vision

"The commitment of the Information Technologies staff is to deliver creative, practical solutions and services in support of the current and future technological needs of El Dorado County."

OUR SERVICES

End User Support

"Customer service is what we do."

- Desktop Support
- Servers Administration
- Network Support
- Email
- Efax
- Internet access

Telecommunications

- Four digit inter-County system dialing
- Local and long distance service
- Voicemail box
- Support and maintenance of County telephone infrastructure
- Provisioning of circuits

Application Development and Support

- Application Development
- Application Support
- Vendor App Management
- Report Writing
- Vendor Interfaces
- Website design and maintenance

Records Management

- Storage
- Retrieval
- Re-Filing
- Records Destruction


FY 18/19 Goals
Application Modernization
Phone System Upgrade
Cloud Utilization

Application Modernization

- FENIX
  - HR/Payroll Live
- Megabyte - Property Tax System Replacement
- Trakit - Land Management / Permitting system
- Recorder Clerk System - SouthTech

Phone System Upgrade

- Core Switch
- Software
- Installation at the new Public Safety Facility

Cloud Utilization

- Our definintion of "Cloud" must be based on strategic plan requirements
- Reduce Total Cost of Ownership
- Gain efficiencies in resources
- Resilient operations, disaster tolerant
- Meets requirement for physically remote backup site
- Requires shift in procurement and contracting - utility pricing model


FY 19/20 Goals
Disaster Recovery
Office 365 Deployment
Security

Disaster Recovery

- IT Service Catalog
  - Requirements gathered (via Readiness Response team's COOP program)
- Recovery Point Objective (How much data can you lose)
- Recovery Time Object (How long can you be down)
- Scenarios to consider
  - Data center disabled or destroyed
  - Fire or other outside disaster (not affecting the data center)
  - System/application/network failures
  - Successful Cyber Attack

Risk Management

What do different risk management cultures look like?

Determine how your organization fits the criteria listed below. Descriptions and examples do not have to match your organization perfectly.

Risk Tolerant

- You have no compliance requirements.
- You have no sensitive data.
- Customers do not expect you to have strong security controls.
- Revenue generation and innovative products take priority and risk is acceptable.
- The organization does not have remote locations.
- It is likely that your organization **does not operate** within the following industries:
  - Finance
  - Health care
  - Telecom
  - Government
  - Research
  - Education

Moderate

- You have some compliance requirements, e.g.:
  - HIPAA
  - PIPEDA
- You have sensitive data, and are required to retain records.
- Customers expect strong security controls.
- Information security is visible to senior leadership.
- The organization has some remote locations.
- Your organization most likely **operates within** the following industries:
  - Government
  - Research
  - Education

Risk Averse

- You have multiple, strict compliance and/or regulatory requirements.
- You house sensitive data, such as medical records.
- Customers expect your organization to maintain strong and current security controls.
- Information security is highly visible to senior management and public investors.
- The organization has multiple remote locations.
- Your organization operates within the following industries:
  - Finance
  - Healthcare
  - Telecom

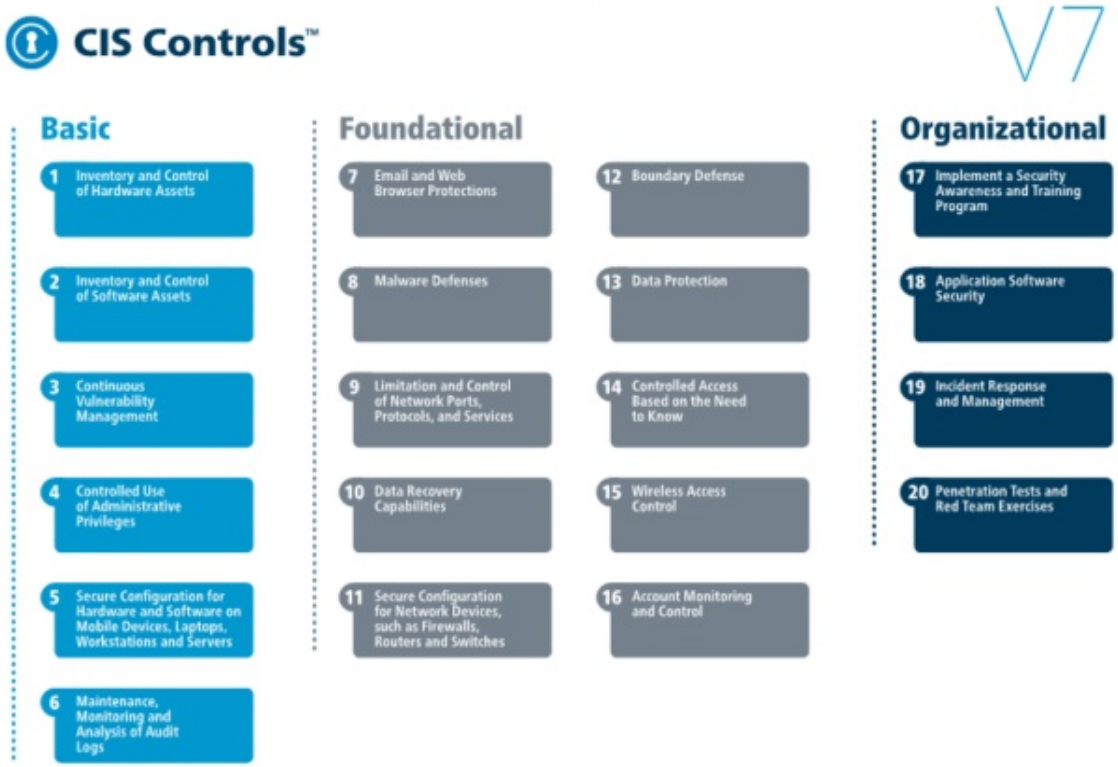
Info-Tech Research Group 7

Where does our organization fit?

Office 365 Deployment

- Office Suite Upgrade
- Email Migration
  - Professional services
- One-Drive, SharePoint, Skype migrations

Security


CIS Controls™
V7
Basic
1 Inventory and Control of Hardware Assets
2 Inventory and Control of Software Assets
3 Continuous Vulnerability Management
4 Controlled Use of Administrative Privileges
5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6 Maintenance, Monitoring and Analysis of Audit Logs
Foundational
7 Email and Web Browser Protections
8 Malware Defenses
9 Limitation and Control of Network Ports, Protocols, and Services
10 Data Recovery Capabilities
11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12 Boundary Defense
13 Data Protection
14 Controlled Access Based on the Need to Know
15 Wireless Access Control
16 Account Monitoring and Control
Organizational
17 Implement a Security Awareness and Training Program
18 Application Software Security
19 Incident Response and Management
20 Penetration Tests and Red Team Exercises