Outdated applications and conversions

Be aware of outdated system risks and be prepared for conversions

Sonya Singh | IT System Assistant Audit Manager
Audrie Shellhart | IT Systems Auditor

Office of the Washington State Auditor

About SAO

State Auditor
Pat McCarthy

- Non Audit Services
  - Center for Government Innovation
  - Technical Support
- Audit Services
  - Performance & IT Audit
  - Special Investigations
  - State & Local Audit

Agenda

Outdated Applications:

- Business critical applications
- Risks with outdated applications
- What to do about these risks

Conversions:

- Selecting a new application
- Moving data
- User access impacts
- Interfacing impacts
- Data backup recovery impacts
- Patch management impacts

What are business essential and mission critical applications?

What is an outdated applications?

- Outdated technology
- No longer supported
- Lack of personnel

Sharing data

SHARING DATA FROM ONE DEPARTMENT TO ANOTHER

SHARING DATA TO OTHER AGENCIES

What are risks related to outdated application?

Risks with outdated application

Increased vulnerability to security threats → Disruption in functionality → Decreased productivity → Not meet standards and compliance

Common Identified Issues

- Not having procedures
- Not performing risk assessments
- Not mitigating and addressing risks

What do you do?

IDENTIFY AND EVALUATE APPLICATIONS

CONDUCT RISK ASSESSMENTS

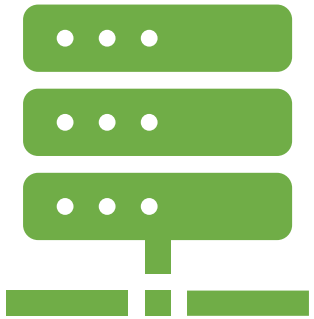
MITIGATE THE RISKS

SAO Resources

Conversions

What's a conversion?

Data moving from one spot to another



Version changes, platform changes, server changes, whole system changes

Selection

- Business needs
- Bidding and compliance requirements
- Similar systems

STAFF PROPERLY TRAINED

NEW CONTROLS

HAVING A PLAN

CREATING A FLOWCHART OF DATA

Data

TRANSACTION HISTORY

RATE TABLES

ACCRUAL RATES

OUTSTANDING BALANCES

CLEAN UP DATA

KNOW WHERE HISTORICAL DATA

RETAIN TESTING DOCUMENTATION

Common issues

Not retaining testing reconciliations/validations → Not having a plan → Not ensuring data is complete and accurate

Software Conversion Resource

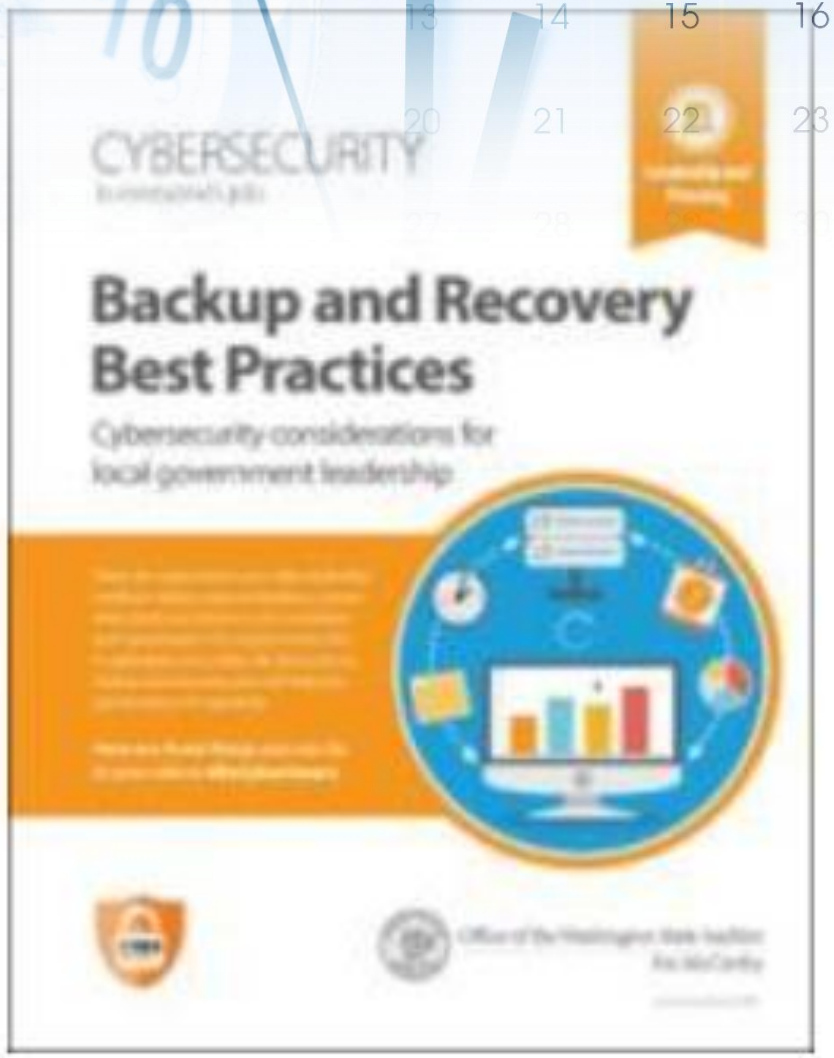
Did you backup?

- Perform backup before and after the conversion
- Re-evaluate existing procedure

Common issues

Lack	Lack of procedures, plans and documentation
Lack	Lack of vendor monitoring
Lack	Lack of test restores

Backup Recovery Resource



How are you going to Patch the new system?

- Who’s responsible for patching? IT or Vendor?

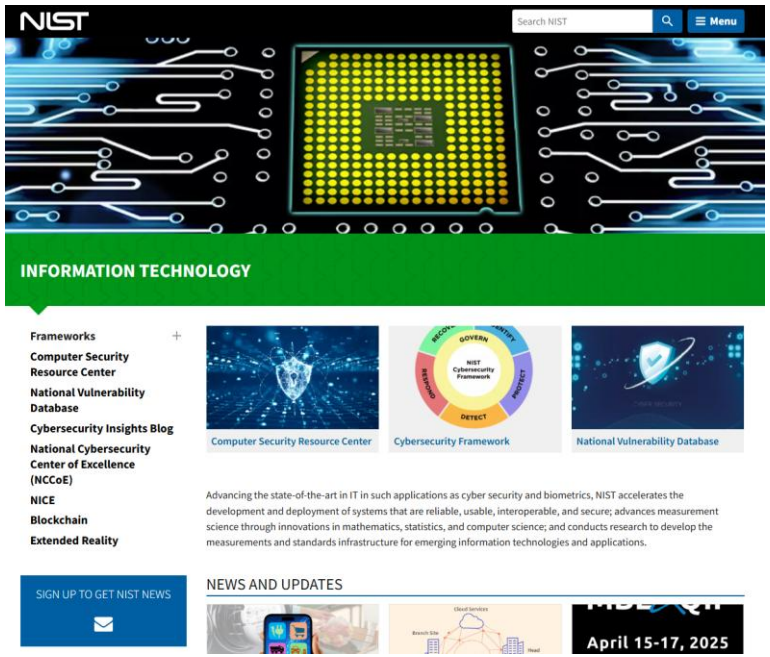
Common issues

LACK OF PROCEDURES

LACK OF MONITORING

LACK OF EVALUATION

Patch Management Resources



Does the system interface to any other applications?

User Access

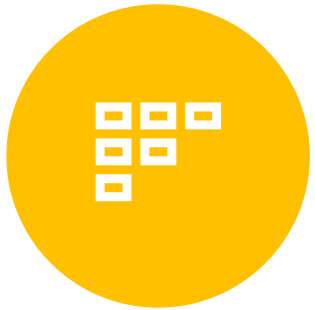
PROTECT DATA

MINIMIZE RISK OF UNAUTHORIZED ACTIVITIES

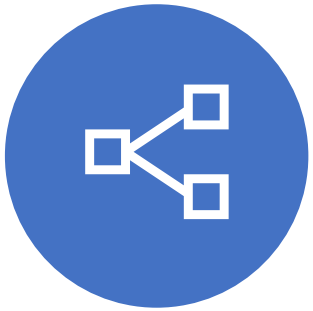
Common issues:

LACK OF POLICIES

LACK OF MONITORING



LACK OF LIMITED ACCESS



LACK OF SEPARATION OF DUTIES

Vendor Management

Monitor activities

Monitor transactions

Monitor data

Vendor Management

- Help with trouble shooting
- Help with data transfer
- Help with service accounts

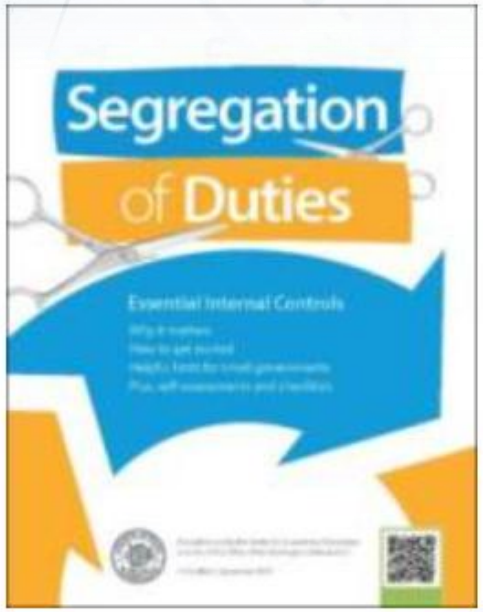
Common issues

NO WRITTEN CONTRACTS

LACK OF MONITORING

LACK OF EVIDENCE


Center for Government Innovation
Improve your cybersecurity without breaking your budget
Office of the Washington State Auditor
Pat McCarthy
Balancing the many needs and budget priorities of your local government is challenging and finding dollars for cybersecurity programs may seem monumental. Would you be surprised to learn there are tools you can use at little to no cost? Here, we have rounded up some of the best resources available to help you improve your cybersecurity posture.
1. Multi-State Information Sharing and Analysis Center (MS-ISAC) offers free membership with many benefits
As a local government, this is your key resource for cyber-threat prevention, protection, response and recovery! MS-ISAC is funded by the Department of Homeland Security, so it has many free and low-cost services, such as immediate help should you experience a cyber-incident. MS-ISAC's operations center is available 24/7, and offers free incident response services like emergency conference calls, mitigation recommendations and forensic analysis.
2. Cybersecurity & Infrastructure Security Agency (CISA), a division of Homeland Security, offers services at no cost
CISA, a division of Homeland Security, offers free services to local governments including vulnerability scanning, phishing campaign assessment, and remote penetration testing. For a complete list of services, see https://www.cisa.gov/cyber-resource-hub.
3. The Public Infrastructure Security Cyber Education System (PISCES) helps small local governments
PISCES connects small municipalities (fewer than 150 network users) with students who analyze live-streaming metadata, and perform network and threat analyses. CISA and Pacific Northwest National Laboratory support PISCES, and it started here in Washington.
March 2022


Segregation of Duties
Essential Internal Controls


CYBERSECURITY
is everyone's job.
Leadership and Planning
It starts with policy
A guide to jump-starting your cybersecurity program
Here are what different groups need from your IT policies to #BeCyberSmart.
Office of the Washington State Auditor
Pat McCarthy

Resources

Summary:

Outdated Applications:

- Identify and evaluate

Conversions:

- Evaluate the application
- data is complete and accurate
- application interfaces
- Perform Backups before and after the conversion
- Ensure patches are monitored
- Perform user access reviews six months after going live and there after according to internal policies

Questions?

Office of the Washington State Auditor

Information

Audrie Shellhart

IT Systems Auditor

Audrie.Shellhart@sao.wa.gov

(564) 201- 2964

Sonya Singh, MS-ITAM
IT Systems Assistant Audit Manager

Sonya.Singh@sao.wa.gov

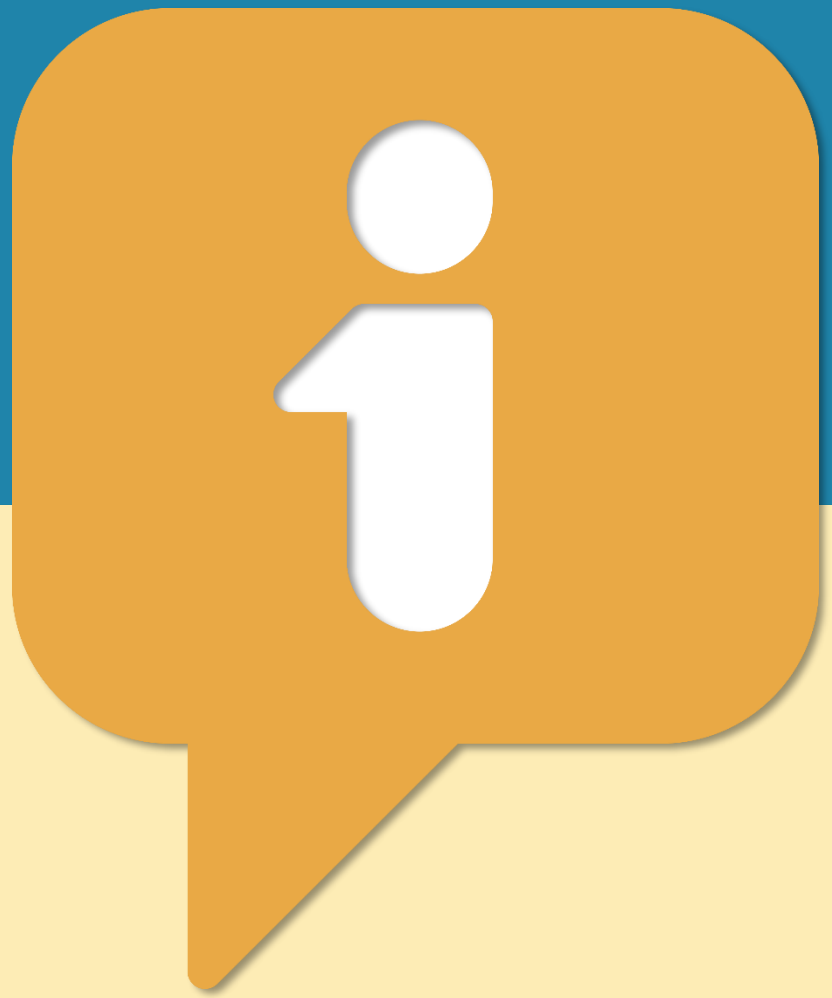
(360) 594-0614

Karen Wilson, CPA, CISA

IT Systems Program Manager

Karen.Wilson@sao.wa.gov

(509) 581-3990



Website: sao.wa.gov
Twitter: @WaStateAuditor
Facebook: facebook.com/WaStateAuditorsOffice