

Consolidated Slides from 11-8-18 Fraud & Cyber-crime Presentations

- FBI: Threat Analysis Slides Not Provided
- Internal Control Reviews Summary Report
- State Auditor: Detecting Fraud (no videos)
- Evolving Controls
- Summary of Risks & Tools

Agenda

- 8:30 Opening by Auditor Greg Kimsey
- 8:35 FBI Cyber Threat Analysis
- 9:30 Internal Control Reviews, 2018
- 9:40 Break
- 9:55 State Auditor Office: Detect Fraud
- 10:50 Evolving Controls
- 11:20 IT Progress Report
- 11:30 Summary of Risk and Tools
- 11:40 Closing by Mark Gassaway

Agenda

- 8:30 Opening by Auditor Greg Kimsey
- 8:35 FBI Cyber Threat Analysis
- 9:30 Internal Control Reviews, 2018
- 9:40 Break
- 9:55 State Auditor Office: Detect Fraud
- 10:50 Evolving Controls
- 11:20 IT Progress Report
- 11:30 Summary of Risk and Tools
- 11:40 Closing by Mark Gassaway



Summary of 2018 Auditor's Unscheduled Internal Control Reviews

Trends, Issues and Recommendations

Tom Nosack, Senior Management Analyst
Clark County Auditor's Office
November 8, 2018 v.2



Phishing
It's not fun for the Phish

Does it matter how it happened?



A loss comes from a variety of sources

- External Attack: Hacking, spoofing, phishing
- Internal Attack: Theft, Fraud, Curiosity
- Internal Error: Poor controls, carelessness, distraction, inadequate separation of duties

Internal Controls

- Effective internal controls are the best tool against **most** risks
- You need to check your internal controls regularly to make sure they are effective.
- Who can you call for help?

Clark County Code

- **Section 2.14** “The auditor is authorized to examine any office, department, political subdivision or organization which receives appropriations from the board of county commissioners.”
- **Section 2.14.030(a):** (The auditor) must “appraise the adequacy and completeness of internal controls”

How much is at risk?

Clark County holds about **\$38,000 to \$40,000** in cash daily – but much more than this passes through the financial system

2017 pass through: over **455,700** transactions in excess of **\$245,000,000**

Bob, the amateur Fish Talker



Bob, the Amateur Fish Talker



Auditors
want to
talk to ME?

Internal Controls Reviews: the ICR

- The ICR is not an audit, but checking internal controls is part of an audit.
- An ICR is a limited review of your group's cash and general security operations.
- The visit may be a cash count, a review of cash handling, security procedures or storage standards.

What to Expect from a Visit

- Auditors arrive and self-identify
- Verify what is on hand for cash account
- Reconcile the account to last statement
- Observe receipting and cash handling
- Discuss internal controls & issues
- Written report in 3-5 days

Recent ICR History

2017

- 22 visits to:
 - Auditor
 - Community Development
 - Community Services
 - Clerk
 - District Court
 - General Services
 - Public Health
 - Public Works
 - Prosecuting Attorney
 - Superior Court
 - Sheriff's Office
 - Treasurer

2018

- 23 visits to:
 - Community Development
 - Community Services
 - District Court
 - General Services
 - Public Works
 - Prosecuting Attorney
 - Sheriff's Office
 - Treasurer

2018 Summary Results

- 28 recommendations from 23 visits
- Overall:
 - Policies and procedures need more attention
 - Management needs more active oversight
 - Decrease variance in daily account balances

Progress on 2017 Problem Areas

2017

- Security of valuables
- Custodian list not accurate
- Written procedures inaccurate
- Too few management reviews
- Cash handling variances

2018

- Improved
- Improved
- No Change
- No Change
- Needs Improvement

Who did well in 2018?



Who did well in 2018?

- 23 visits to:
 - Community Development
 - Community Services
 - District Court
 - General Services
 - Public Works
 - Prosecuting Attorney
 - Sheriff's Office
 - Treasurer
- Two Tactical Detectives
Unit Funds
- Two Drug Task Force
Funds
-
- ```
graph LR; A[Two Tactical Detectives Unit Funds] --> B[Sheriff's Office]; C[Two Drug Task Force Funds] --> B;
```

# A real Fish Talker...



**...doesn't need a  
fishing pole**



# Summary

- We can help you with planning, deploying, and testing of internal controls
- Visits are on a three year rotation, but...
- Actual visits will vary based on risk

A happy fish...



...isn't on the end of a line - Thank You!



Office of the Washington State Auditor

---

Pat McCarthy

# Cybersecurity risks: A local government perspective

**Aaron Munn, CISSP, ISRM, MSCE – IT Security Team Manager**



# Learning objectives

- Role of Auditor's Office in cybersecurity
- Weapons and tactics used against local governments
- Detecting and defending against cyberattacks

# Part 1

## State Auditor's Office Role

# State Auditor's Office role in cybersecurity

- Audit programs
  - Performance audits
  - Attestations
  - Accountability
  
- Performance Center collaboration
  - **Phase 1:** Develop a list of desired resources and determine if they already exist or need to be developed in-house
  - **Phase 2:** Evaluate resources that already exist and communicate their availability
  - **Phase 3:** Develop selected new resources, and post and communicate their availability



# Cybersecurity risk assessment

- How the Auditor's Office does it
- An “all-in” approach
- Third-party assistance
- Relationships between departments

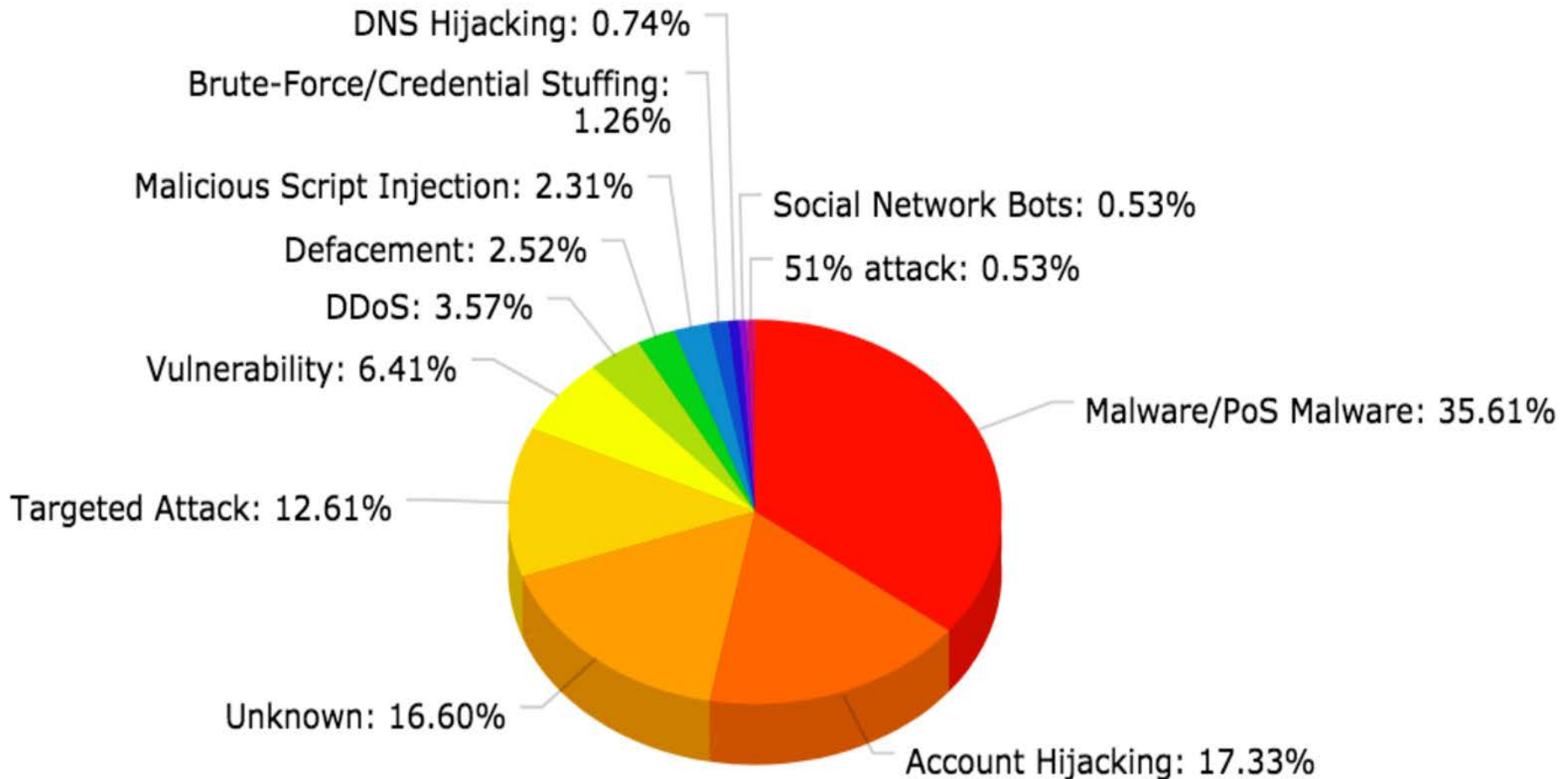


## **Part 2**

**Weapons and tactics  
used against local governments**

# Hackmageddon statistics

## Attack Distribution (Top 10 2018)



# Malicious actors

 **WANTED  
BY THE FBI**

**CONSPIRACY TO COMMIT COMPUTER INTRUSIONS; CONSPIRACY TO COMMIT WIRE FRAUD; COMPUTER FRAUD - UNAUTHORIZED ACCESS FOR PRIVATE FINANCIAL GAIN; WIRE FRAUD; AGGRAVATED IDENTITY THEFT**

|                                                                                    |                                                                                    |                                                                                     |                                                                                      |                                                                                     |
|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|   |   |   |   |  |
| Gholamreza Rafatnejad                                                              | Ehsan Mohammadi                                                                    | Seyed Ali Mirkarimi                                                                 | Abdollah Karima                                                                      | Mostafa Sadeghi                                                                     |
|  |  |  |  |                                                                                     |
| Sajjad Tahmasebi                                                                   | Mohammed Reza Sabahi                                                               | Roozbeh Sabahi                                                                      | Abuzar Gohari Moqadam                                                                |                                                                                     |

**CAUTION**

On February 7, 2018, a grand jury sitting in the United States District Court for the Southern District of New York, indicted nine Iranian nationals for their alleged involvement in computer intrusion, wire fraud, and aggravated identity theft offenses. As alleged in the indictment, the men were involved in a scheme to obtain unauthorized access to computer systems, steal proprietary data from those systems, and sell that stolen data to Iranian customers, including the Irania: **federal and state government agencies** each individual was a leader, contractor, associate, hacker for hire, or affiliate of the Mabna Institute, a private government contractor based in the Islamic Republic of Iran that performed this work for the Iranian government, at the behest of the Islamic Revolutionary Guard Corps. Victims of the scheme included approximately 144 universities in the United States, 176 foreign universities in 21 countries, five federal and state government agencies in the United States, 36 private companies in the United States, 11 foreign private companies, and two international non-governmental organizations.

**THESE INDIVIDUALS SHOULD BE CONSIDERED AN INTERNATIONAL FLIGHT RISK**  
If you have any information concerning this case, please contact your local FBI office, or the nearest

# Ransomware

**Cause:** System misconfiguration / possible phishing attack

**Risk:** Public safety

**Possible cost:** Reduced response times  
for first responders

**Value to thief:** High payback if successful



# Ransomware

KSL.com



## Hackers demand \$25K-\$30K after ransomware attack takes down county's servers in Idaho

By Stephan Rockefeller, EastIdahoNews.com | Posted Feb 17th, 2017 @ 7:34pm



BLACKFOOT, Idaho — Bingham County, Idaho officials are still scrambling to rebuild parts of their computer infrastructure after a ransomware attack took down county servers on Wednesday.

Although efforts have been made to correct the problem, computer issues remained as of Friday.

“Every department in the county is affected in some way,” Bingham County Commissioner Whitney Manwaring told [EastIdahoNews.com](http://EastIdahoNews.com). “Phone systems, computer systems, everything. Some departments are handwriting documents.”

# Data breach

**Cause:** Employee misuse

**Risk:** Loss of confidential employee records

**Possible cost:** 250,000 records x \$75 = \$18 million

**Value to thief:** Access to confidential records

# Data breach

## Adams County clerk resigns after data breach that affected up to 250,000 people

Karen Madden, Wisconsin Rapids Daily Tribune

Published 4:21 p.m. CT Sept. 19, 2018



(Photo: Courtesy Cindy Phillippi)

[f](#) CONNECT | [TWEET](#) | [LINKEDIN](#) | [COMMENT](#) | [EMAIL](#) | [MORE](#)

FRIENDSHIP - The Adams County clerk has resigned her position, effective as of the end of 2018, and will be on a paid leave of absence for the rest of the year, according to an agreement signed Tuesday.

The resignation comes after a data breach that affected up to 250,000 people was announced by Adams County on Aug. 10. The Adams County Board had been investigating Clerk Cindy Phillippi's role in the data breach, according to county

# Spear-phishing

**Cause:** Successful phishing attack

**Risk:** Targeting government accounts (usernames and passwords)

**Possible cost:** Currently under investigation

**Value to thief:** Easier than ransomware,  
access to address book and  
government network

# Spear-phishing

Sat 10/20/2018 5:46 PM

McMahon, 

Re: Help Desk

To

 If there are problems with how this message is displayed, click here to view it in a web browser.

---

Your account is been updated due to the recent system configuration.  
To avoid any disruption of service, please [CLICK HERE](#) and follow the instruction.

We apologize for the short notice, disruption, and inconvenience that this will cause.

Yours faithfully,  
Help Desk Department

# Business email compromise

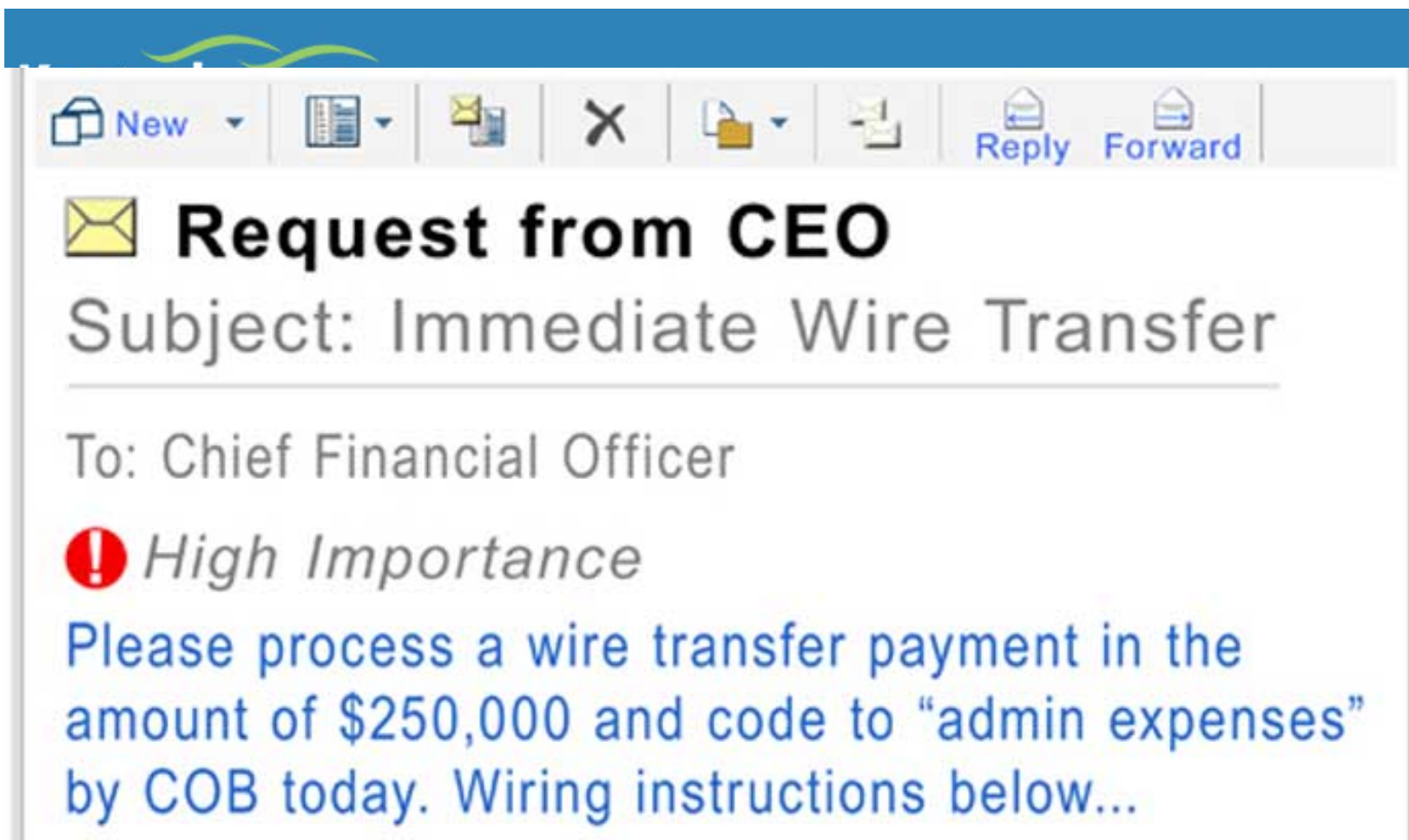
**Cause:** No or ineffective internal controls

**Risk:** Loss of funds (theft)

**Possible cost:** Average loss for BEC victims is \$130,000,  
according to FBI

**Value to thief:** Simple, low overhead, quick return

# Business email compromise



# Phishing attack and data breach

**Cause:** Successful phishing attack

**Risk:** Data breach

**Cost:** Commissioners approved paying \$5,000  
for the insurance deductible

**Value to thief:** High return on investment



# Phishing attack and data breach



## County data breach from email scam

By TESS NOVOTNY H&N Staff Reporter Jul 25, 2018

Tired of seeing surveys on articles? If you are a subscriber, simply

[log in](#)

or

[Subscribe now!](#)



Klamath County commissioners approved a \$5,000 deductible agreement with Portland-based data security firm ID Experts to investigate and respond to a county employee data breach that occurred on July 9.



Klamath County discovered that two employees clicked a link in a mass phishing scam email that prompted employees to share their county credentials and sign an online document.

# Business email compromise

**Cause:** Employee sent confidential information to fake City administration email account

**Risk:** Data breach

**Possible cost:** Fraud protection for hundreds of employees, reputational harm

**Value to thief:** Multiple victims, high financial return

# Business email compromise

Manually run video # z1 now

# Business email compromise

**Cause:** Business email compromise

**Risk:** Loss of funds

**Cost:** \$49,284

**Value to thief:** Low risk, quick result

# Business email compromise

## Stephan Lagerholm

Notes from a councilman in Yarrow Point

MENU



## New IT-Security incident at Yarrow Point

On Friday I was notified about another IT-Security related incident that the Town fell victim for. So far not much information is available, but it appears that the attack resulted in some files and systems being inaccessible. Below is the notification that was sent from the Town. The Town also updated their website with information about the incident.

# Business email compromise

**Cause:** Employee clicked link in email

**Risk:** Ransomware attack

**Cost:** Almost \$10,000

**Value to thief:** Low risk, quick result

# Business email compromise

## Wire-transfer scheme, ransomware attack — tiny Yarrow Point finds itself in criminals' crosshairs



Originally published February 25, 2018 at 8:00 am Updated March 1, 2018 at 1:17 pm



Source: Esri

MARK NOWLIN / THE SEATTLE TIMES

2 of 2

# Email spoofing, a simple proposition

Manually run video # z2 now



# Victim response actions

- “... more training for staff using county computers.”
- Paid the ransom
- “... no longer allowing wire transfers and switching and updating equipment and systems like email.”
- “... offered to pay for fraud protection (for employees)...”
- “... only paying the cyber security insurance deductible amount.”
- “... closed the ability for employees to access work email from home about a week ago.”

# Part 3

## Detecting and defending against cyberattacks

# Protect Your Password

Manually run video # z3 now



**Cyber Security**

is everyone's  
responsibility...

**Protect your information**

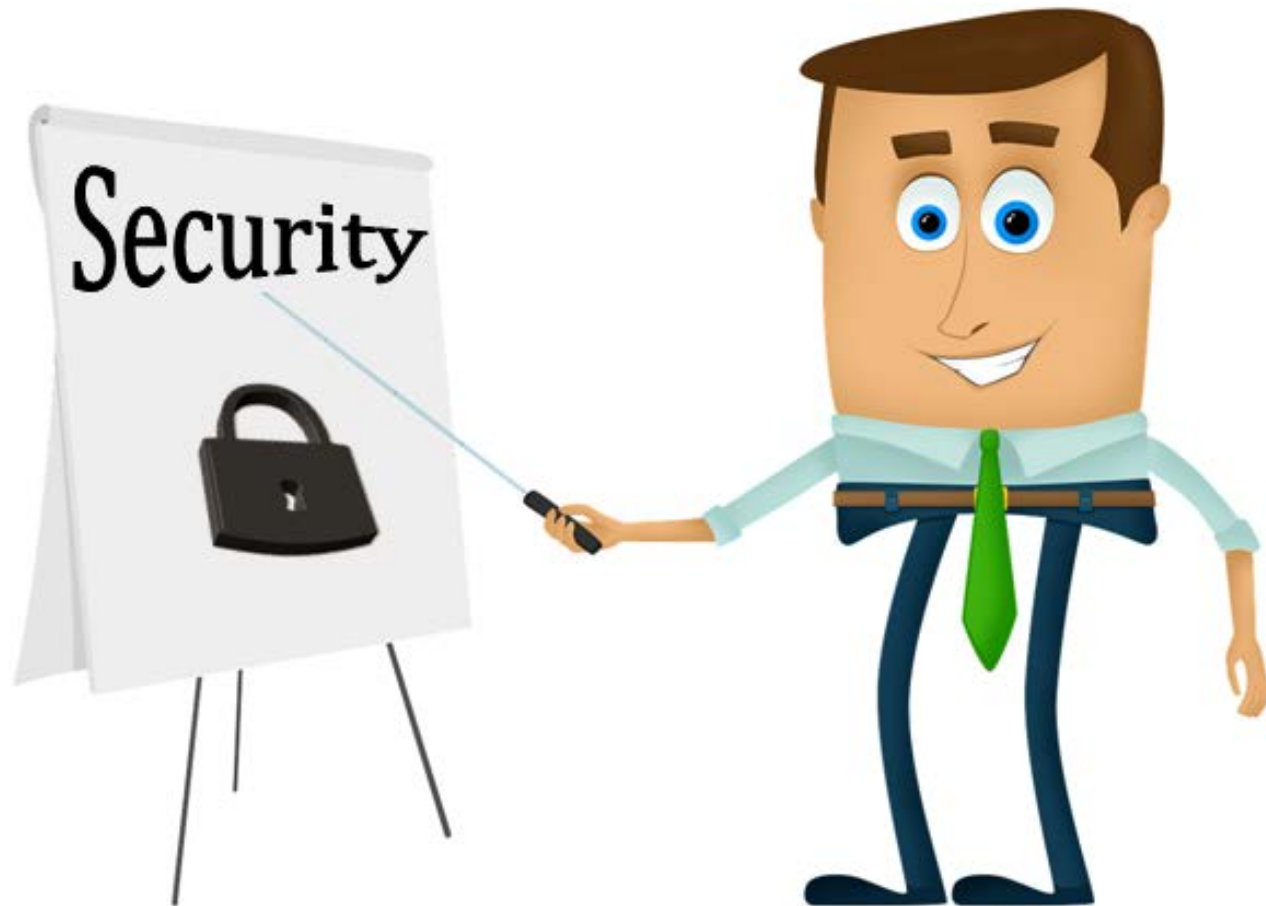
at home and at work!



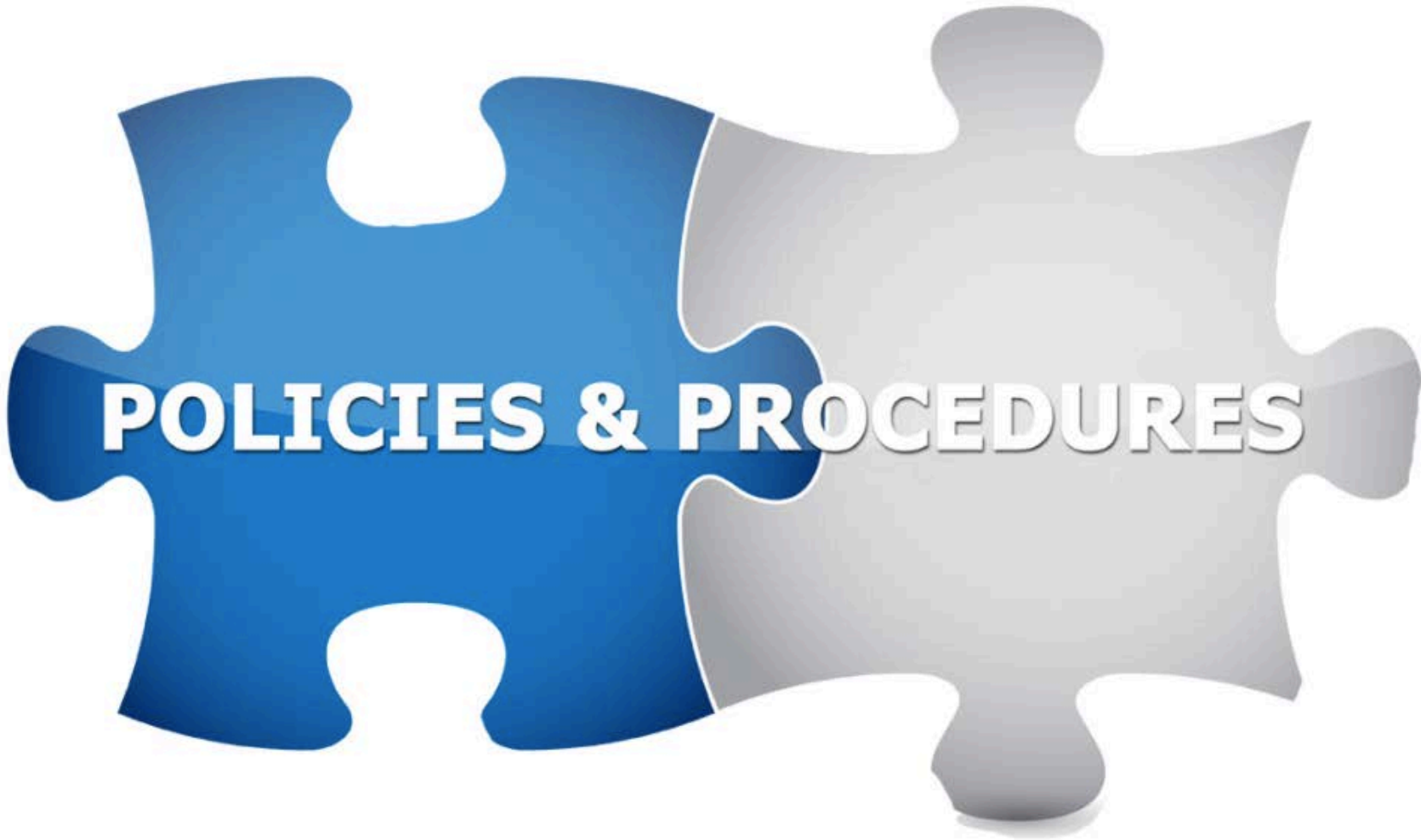
# Protect your digital footprint

The image shows a screenshot of the Washington State Auditor's website. The browser address bar displays <http://www.sao.wa.gov/about/Pages/ContactUs.aspx>. The page header includes the Auditor of State logo and navigation links: About Us, Local Government, State Government, Investigations, Resources, and Search. A search bar is located in the top right corner. The main content area is titled "Contact Us" and contains contact information for the Main Office, including the address (302 Sid Snyder Way, Olympia, WA 98512) and phone number (360) 902-0333. A sidebar menu on the left lists: About Us, State Auditor Pat McCarthy, Mission and Goals, Who Audits the Auditor?, Careers, Contact Us, and Audit Dispute Process. A large, colorful cluster of social media icons is overlaid on the page, including Facebook, WhatsApp, LinkedIn, YouTube, Instagram, Twitter, and many others.

# Security awareness and training



# Documentation





# The bottom line



# Contacts

## **Pat McCarthy**

State Auditor

(360) 902-0360

[Auditor@sao.wa.gov](mailto:Auditor@sao.wa.gov)

## **Peg Bodin, CISA**

Assistant Director of IT Audit

(360) 464-0113

[Peggy.Bodin@sao.wa.gov](mailto:Peggy.Bodin@sao.wa.gov)

## **Aaron Munn, CISSP, ISRM, MSCE**

IT Security Team Manager

(360) 725-5418

[Aaron.Munn@sao.wa.gov](mailto:Aaron.Munn@sao.wa.gov)

Websites: [www.sao.wa.gov](http://www.sao.wa.gov)

[auditconnectionwa.org](http://auditconnectionwa.org)

Facebook: [www.facebook.com/WAStateAuditorsOffice](http://www.facebook.com/WAStateAuditorsOffice)

Twitter: [www.twitter.com/WAStateAuditor](http://www.twitter.com/WAStateAuditor)



# EVOLVING TECHNOLOGY AND THE DEMANDS ON YOUR INTERNAL CONTROLS

ARNOLD PÉREZ



# Classic Fraud Charges to Accounts

- Check Fraud
- Bogus Debit Card Transactions
- Fraudulent Warrants



# 30-Day Rule for Checking Accounts

- The U.S. Uniform Commercial Code states that organizations issuing checks normally have a responsibility to notify the bank about check fraud no later than 30 days after the closing business date shown on the bank statement.
- Organizations should implement procedures to promptly identify check fraud thus improving the chances of a successful prosecution of the perpetrator.
- All organizations should review the bank statements and their enclosures immediately upon receipt to identify any fraudulent financial transactions such as bogus checks, debit card transactions, or warrants.



# 24 Hour Rule for Debit Card Transactions

- The U.S. Uniform Commercial Code states that governments, private businesses, and individuals have a short time span to report bogus debit card transactions posted on their bank statements; they must act within 24 hours of the posting.
- Waiting for the monthly bank statement to arrive simply isn't good enough when it comes to avoiding losses from bogus debit card transactions.
- Organizations that ignore this 24-hour rule suffer the consequence of losses of funds with no possibility of a claim against the bank for reimbursement when bad debit card transactions occur.



# 24-Hour Rule for Warrants



- The U.S. Uniform Commercial Code also applies to warrants. Warrants move through the banking system just like checks until they reach the organization's bank.
- Government agencies must report fraudulent warrants to their banks within 24 hours of presentation.
- If the government fails to pick up warrants promptly at the bank and allows the 24-hour period to expire, or if it fails to report warrant fraud to the bank within 24 hours, the bank will deny any claim for losses.
- In those circumstances, bogus warrants automatically become the responsibility of the government, which sustains a loss of treasury funds.



# What measures can you take?

- Account Reconciliations
  - Required by the Office of the Washington State Auditor (SAO) Budget, Accounting and Reporting System (BARS)
  - Periodically reviewed by the by the Clark County Auditor's Office, and
  - As a matter of necessity for fighting fraud!





# BARS 3.8.8: Imprest, Petty Cash and Other Revolving Funds

- SAO provides guidance on the various accounts and covers:
  - Purpose
  - Budgeting
  - Accounts
  - **Controls**
  - Reporting



# BARS: 3.8.8.20.2



- 2. The governing body or its delegate must appoint one custodian of each petty cash account who should be independent:
  - of invoice processing,
  - check signing,
  - general accounting and
  - cash receipts functions.....



# BARS: 3.8.8.20.4



- 4. On at least monthly basis, the fund should be:
  - reconciled to the authorized balance and
  - to the actual balance per bank statements or
  - a count of cash on hand.
- If this reconciliation is done by the custodian, it should be checked or re-performed periodically by someone other than the custodian.
- It is recommended that independent checks **not be scheduled** with the custodian but be done on a **surprise** basis.



# Internal Controls: Bank Reconciliation

- An independent party should receive the unopened bank statement directly from the bank and promptly perform the bank reconciliation
- All redeemed checks should accompany the monthly bank statement so the reviewer can identify check fraud and other check alterations by outsiders and unauthorized checks issued by insiders



# Internal Controls: Bank Reconciliation

- The independent reviewer should reconcile the bank statement with the organization's accounting records immediately upon receipt
- The owner or other designated independent party should verify and sign off on the completed bank reconciliation with his or her signature and the date of the review



# Evolving Types of Fraud

- Account-takeover fraud
- Mobile Fraud:
  - Remote Deposit Capture (RDC)
  - Bluetooth
  - Apps
- Business E-mail Compromise (BEC)



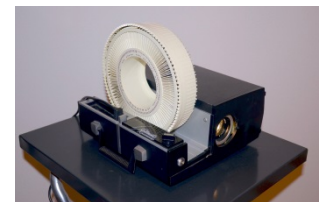
# Commercially Reasonable Security Protocol



# Internal Controls: Review Terms & Conditions



- Commercial business account holders have less time to report cases of fraud, and have more liability and less protection as compared to personal account holders.
- *“We will have no liability to you for acting upon any application, amendment or other communication purportedly transmitted by you, even if such application, amendment or message:*
  - *Contains inaccurate or erroneous information*
  - *Constitutes unauthorized or fraudulent use of Electronic Trade Service*
  - *Includes instructions to pay money, or otherwise debit or credit any account*
  - *Relates to disposition of any money, securities or documents*
  - *Purports to bind you to any agreement or other arrangement with us or with other persons or to commit you to any other type of transaction or arrangement.”*
- Read your own bank’s terms and conditions!





# Internal Controls: Response Plan



- Internet Crime Complaint Center (IC3) & Federal Bureau of Investigation (FBI)
- Public Service Announcement: I-082715a-PSA
- If funds are transferred to a fraudulent account, it is important to act quickly:
  - Contact your financial institution immediately upon discovering the fraudulent transfer.
  - Request that your financial institution contact the corresponding financial institution where the fraudulent transfer was sent.
  - Contact your local Federal Bureau of Investigation (FBI) office if the wire is recent. The FBI, working with the United States Department of Treasury Financial Crimes Enforcement Network, might be able to help return or freeze the funds.
  - File a complaint, regardless of dollar loss, with [www.IC3.gov](http://www.IC3.gov).



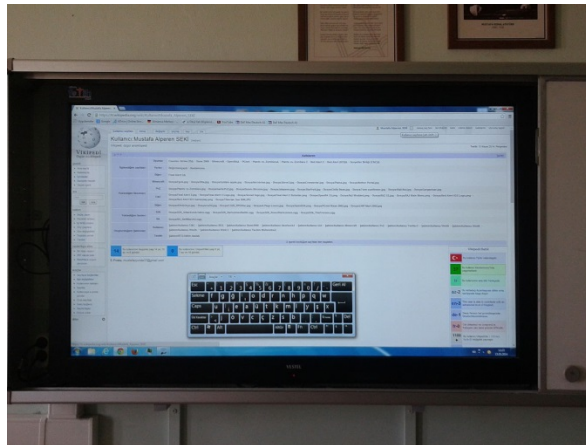
# Internal Controls: Reporting Plan

- Reporting Losses & Thefts at Clark County
  - Notify a Manager- there is no minimum dollar amount - any loss of cash, equipment or materials needs to be reported promptly.
  - Formal police or Sheriff's report must be made, the Audit Services staff will need the police report number.
  - Contact Audit Services- state law requires that we report theft and losses to the State Auditor's Office



# Internal Controls: Training

- Constantly educate staff about cutting-edge fraud techniques
- Don't keep rehashing old security awareness materials and expect to stop online fraud
- Update your training as often as you update your smartphone
- The best training is brief, frequent and focused on the issue at hand



# Internal Controls: Risk Assessment



- Review existing processes, procedures and separation of duties for financial transfers and other important transactions such as sending sensitive data in bulk to outside entities
- Add extra controls, if needed
- Remember that separation of duties and other protections may be compromised at some point by insider threats, so risk reviews may need to be redone



| QUESTIONS                                                                                                  | RESPONSE                                                                                                                                                                                                                                | RISK LEVEL |
|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| Is this a new customer?                                                                                    | No                                                                                                                                                                                                                                      | 0          |
| Have we completed and received payment for less than five orders with this customer in the past two years? | Yes                                                                                                                                                                                                                                     | 1          |
| Is the quote or order over \$100,000?                                                                      | No                                                                                                                                                                                                                                      | 0          |
| Is there a new supplier associated with this quote or order?                                               | No                                                                                                                                                                                                                                      | 0          |
| Have we processed less than five orders with this supplier/vendor in the past two years?                   | No                                                                                                                                                                                                                                      | 0          |
| Has the customer stated their intent to export or ship the order outside the continental U.S.?             | No                                                                                                                                                                                                                                      | 0          |
| Is the supplier/vendor located outside of the U.S.?                                                        | No                                                                                                                                                                                                                                      | 0          |
| TOTAL                                                                                                      |                                                                                                                                                                                                                                         | 1          |
| Assessed Risk Level                                                                                        | <div style="display: inline-block; width: 100px; height: 15px; border: 1px solid black; position: relative;"><div style="position: absolute; left: 0; top: 0; bottom: 0; right: 0; background-color: #90EE90; width: 10%;"></div></div> | 14%        |



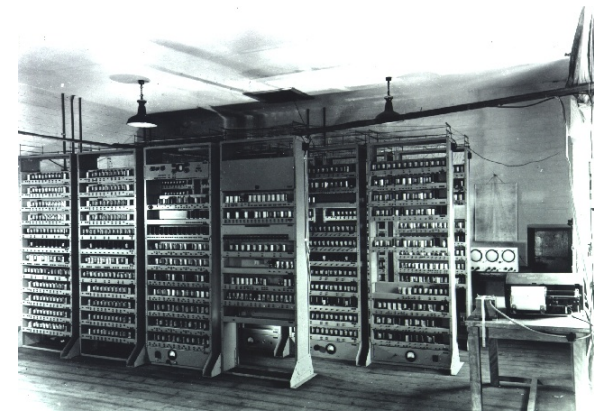
# Internal Controls: P&Ps

- Consider new policies related to “out of band” transactions or urgent executive requests
- An email from an executive’s Gmail or Yahoo account should automatically raise a red flag to staff members, but they need to understand the latest techniques being deployed by the dark side
- You need authorized emergency procedures that are well understood by all

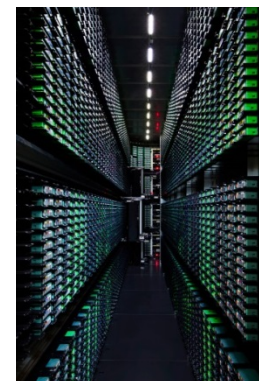


# Internal Controls: Exercises & Communication

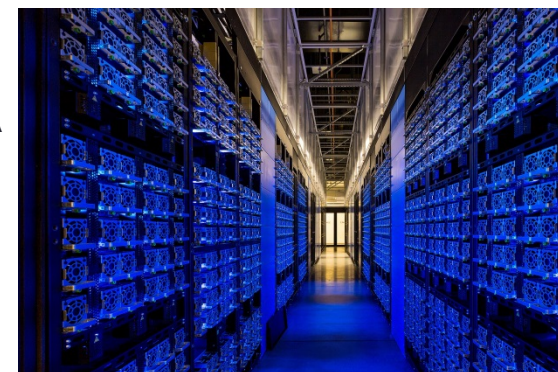
- Review, refine and test your incident management and phishing reporting systems
- Conduct a tabletop exercise with management, including key personnel, on a regular basis
- Test controls and encourage staff recommendations
- Remember, online criminals are always changing and adapting their sophisticated attacks
- Are you ready?



# Resources



- Clark County Auditor's Office
  - <https://clarknet.clark.wa.gov/audit-services/reporting-losses-thefts>
- Office of the Washington State Auditor- Budget, Accounting and Reporting System (BARS) [www.sao.wa.gov](http://www.sao.wa.gov)
- Association of Certified Fraud Examiners [www.acfe.com](http://www.acfe.com)
- Case History Applications, Cash Disbursement Fraud, Authorization and Approval (Part 1 thru 4)
  - May/June 2008 by Joseph R. Dervaes, CFE, ACFE Fellow, CIA
  - July/August 2008 by Joseph R. Dervaes, CFE, ACFE Fellow, CIA
  - September/October 2008 by Joseph R. Dervaes, CFE, ACFE Fellow, CIA
  - November/December 2008 by Joseph R. Dervaes, CFE, ACFE Fellow, CIA
- FBI <https://www.ic3.gov/media/2015/150827-1.aspx>
- Government Technology
  - <http://www.govtech.com/security/GT-July-2017-3-Ways-to-Stop-Business-Email-Compromise.html>
- National Public Radio- All tech considered
  - <https://www.npr.org/sections/alltechconsidered/2015/09/15/440252972/when-cyber-fraud-hits-businesses-banks-may-not-offer-protection>





Thank you!

Arnold Pérez, MPA, CFE, CGAP  
Performance Auditor  
Clark County Auditor's Office  
[Arnold.Perez@clark.wa.gov](mailto:Arnold.Perez@clark.wa.gov)





# CLARK COUNTY INFORMATION TECHNOLOGY

---

Sheri Rugh

Technology Services Director



# Summary of Risks and Tools

Larry Stafford, Audit Services Manager  
Clark County Auditor's Office

|      |             |        |    |
|------|-------------|--------|----|
| 2017 | Montgomery  | County | AL |
| 2018 | Dawson      | County | AL |
| 2018 | Los Angeles | County | CA |
| 2018 | Monroe      | County | FL |
| 2018 | Palm Beach  | County | FL |
| 2018 | Coweta      | County | GA |
| 2017 | Bingham     | County | ID |
| 2018 | Madison     | County | ID |
| 2018 | Davidson    | County | NC |
| 2018 | Onslow      | County | NC |
| 2017 | Multnomah   | County | OR |
| 2018 | Sevier      | County | TN |
| 2018 | Enumclaw    | City   | WA |
| 2018 | Longview    | Port   | WA |
| 2018 | Yakima      | County | WA |
| 2018 | Yarrow (#1) | City   | WA |
| 2018 | Yarrow (#2) | City   | WA |
| 2018 | Adams       | County | WI |
| 2018 | Manitowoc   | County | WI |

# Other Risks: Traditional Fraud

26 fraud reports issued by SAO (2017 -18)

- Misappropriation, personal use of funds
- Payroll, overpayments
- Failure to safeguard funds held in trust (donations)
- Theft of time

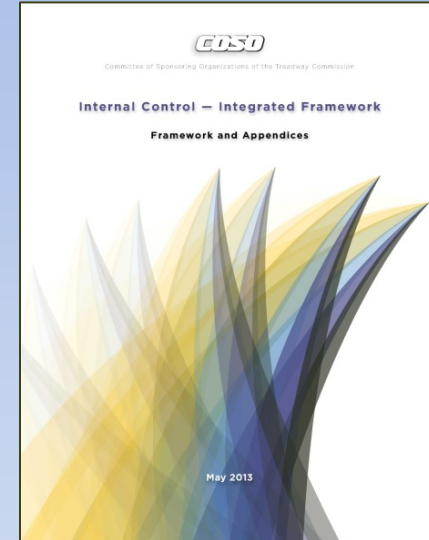
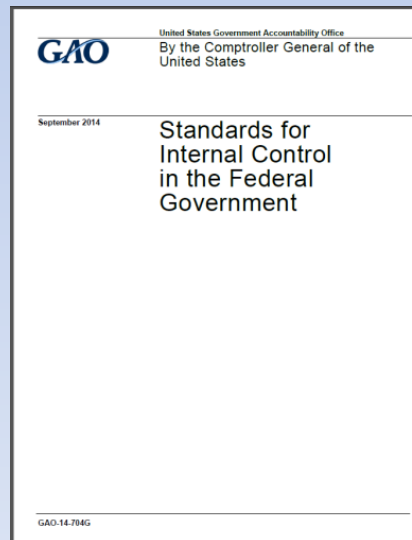
# Other Risks: Traditional Fraud

## Common Control Weaknesses

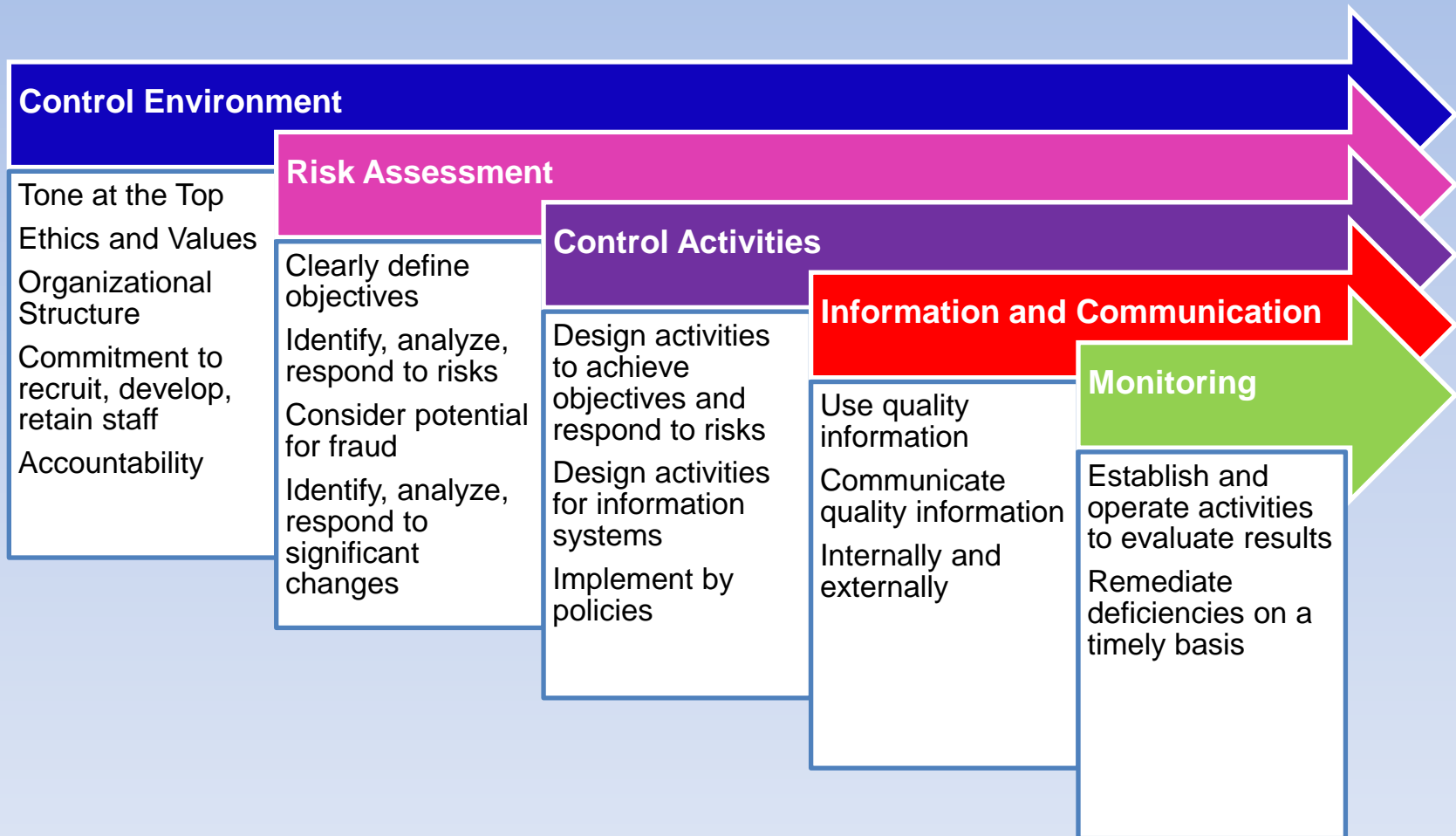
- Lack of segregation of duties
- No independent review
- Incorrect reconciliation process
- Unsecure safe

# Everyone has a role in controls

1. Design
2. Implementation
3. Operating



# Internal Control Framework



*“It is not the strongest of the species that survives, nor the most intelligent, but the one most responsive to change”*

- Leon C. Megginson



Report to Audit Services any:  
Loss of County assets;  
Known or suspected fraud

[arnold.perez@clark.wa.gov](mailto:arnold.perez@clark.wa.gov)

[tom.nosack@clark.wa.gov](mailto:tom.nosack@clark.wa.gov)

[larry.stafford@clark.wa.gov](mailto:larry.stafford@clark.wa.gov)

Thank you!