Virginia Information Technologies Agency

2018 Agency Data Points

Ed Miller
Director IT Security Governance
Joy Young
Information Assurance Analyst

2019 COV Security Conference
April 11, 2019

Agenda

- Overview
- Information Security Governance
- IT Risk Management
- Threat Management
- CSRM Security Services
- NCSR Survey
- Summary

Code of Virginia

As directed by §2.2-2009 (B.1) of the Code of Virginia, the CIO is required to report the:

"results of security audits, the extent to which security policy, standards, and guidelines have been adopted by executive branch and independent agencies, and a list of those executive branch agencies and independent agencies that have not implemented acceptable security and risk management regulations, policies, standards, and guidelines to control unauthorized uses, intrusions, or other security threats."

Code of Virginia

To create this report, CSRM monitors each agency's overall compliance with IT audit program and information security risk program standards and policies.

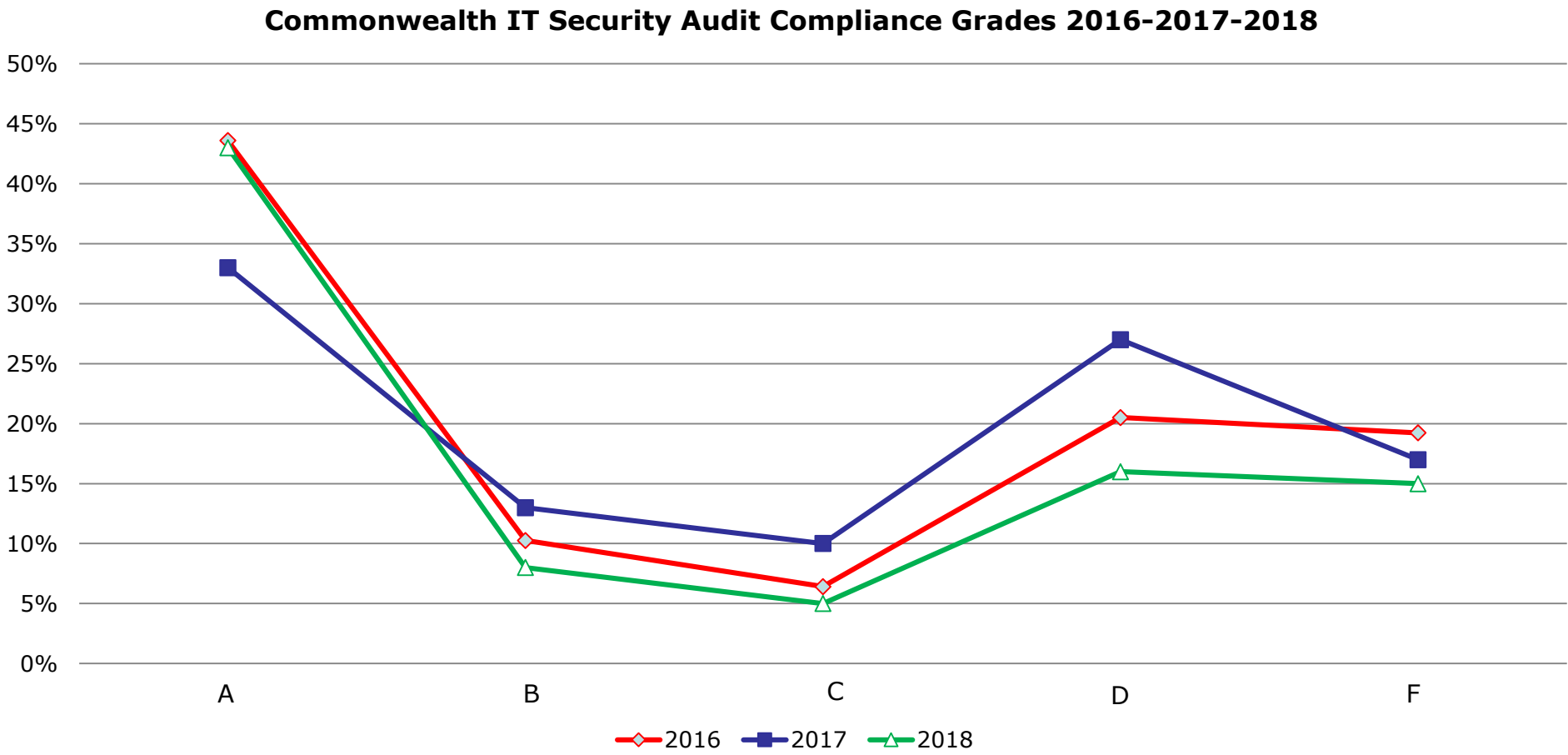
In addition CSRM started transitioning toward a maturity model which provides additional insight into agency programs. This insight will help show where the commonwealth can direct efforts to further the security program.

Agency Compliance Report Card

- The compliance report card summarizes agency compliance with the commonwealth's IT security standards, specifically the standards related to IT security audit and risk management.

- The report card measures each agency's compliance with a letter grade of A, B, C, D, or F to provide a more gradated measurement of agency compliance and more insight into changes in compliance over time.

Compliance Report Card



Agency Audit Programs

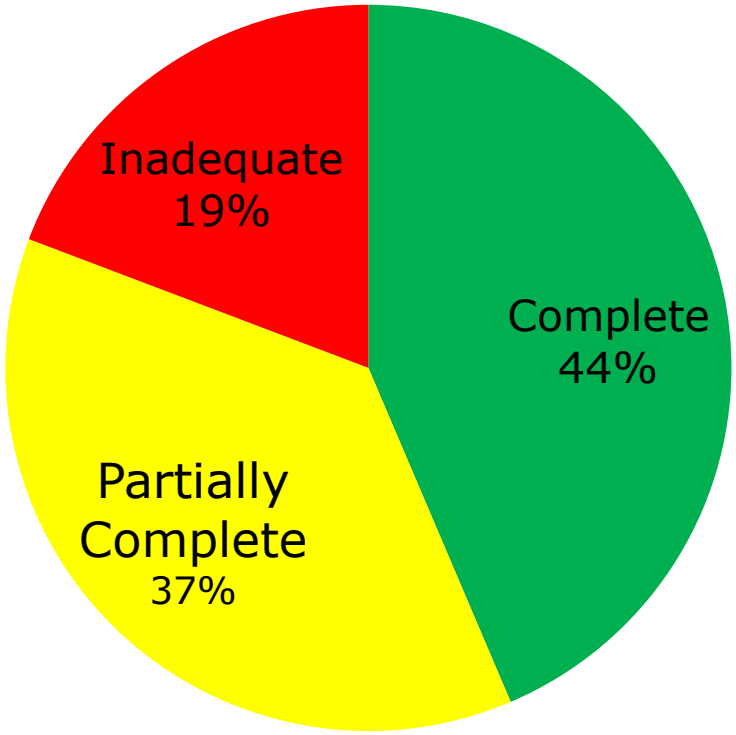
Agencies are required to develop an IT security audit plan annually, conduct IT security audits on sensitive systems, and carry out corrective action plans for findings noted during the audits.

- Audit Plan must be submitted annually
- Sensitive Systems must be audited every 3 years
- Corrective Action Plans must be submitted quarterly

Audit Program Compliance

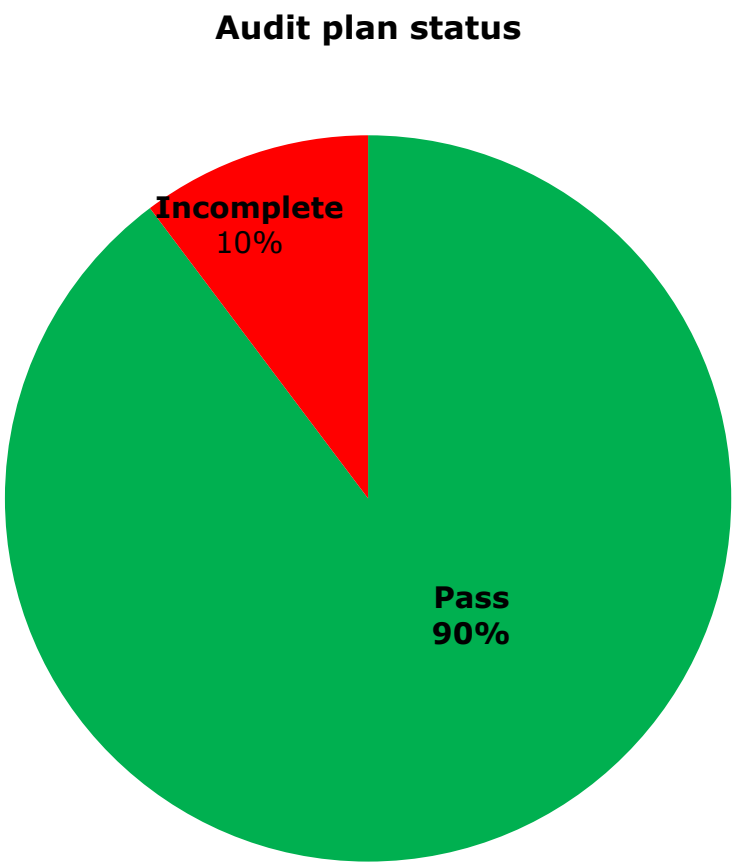
Audit program compliance has improved from the prior year, with 44 percent of agencies having implemented a comprehensive audit program in 2018, compared to 33 percent of agencies with a complete audit program last year.

Audit Program Compliance



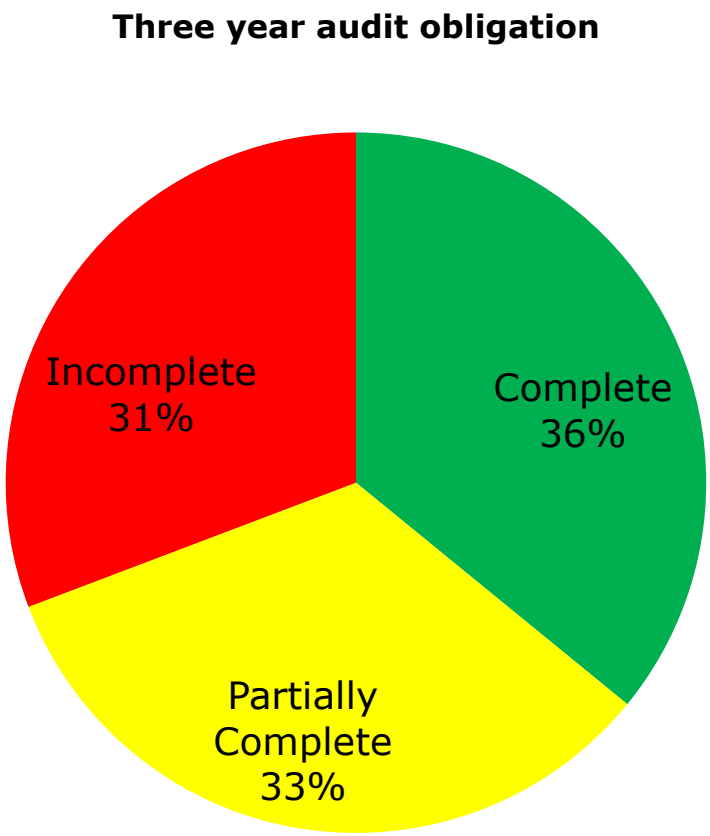
Audit program compliance improved by 11 %

Audit Plan Status



Three Year Audit Obligation

Three year audit obligation completions increased by 8 percent

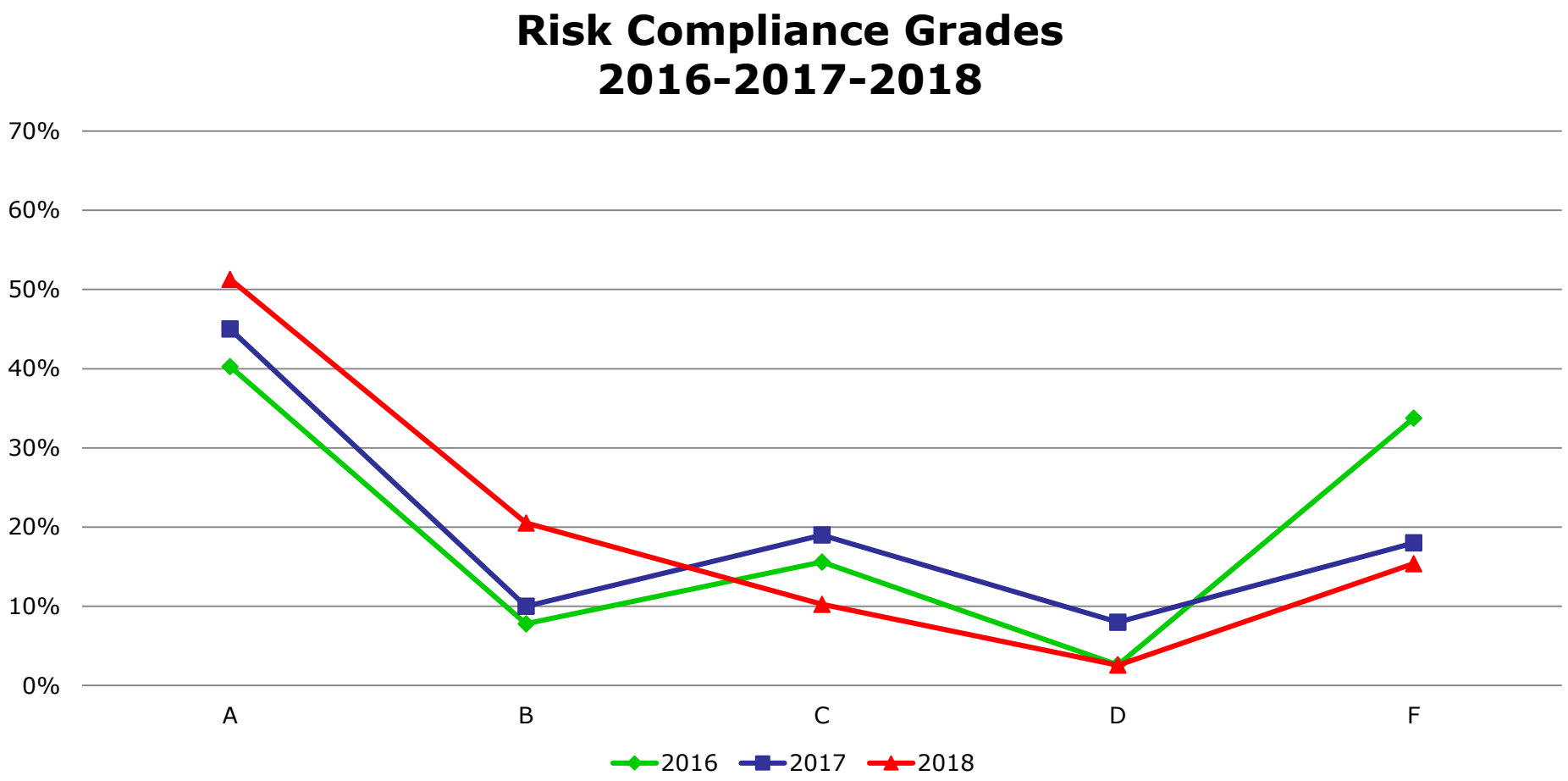


IT Risk Management Program

CSRM reviews agency oversight of their risk management programs. The data we analyze is used to develop each agency's overall risk program score.

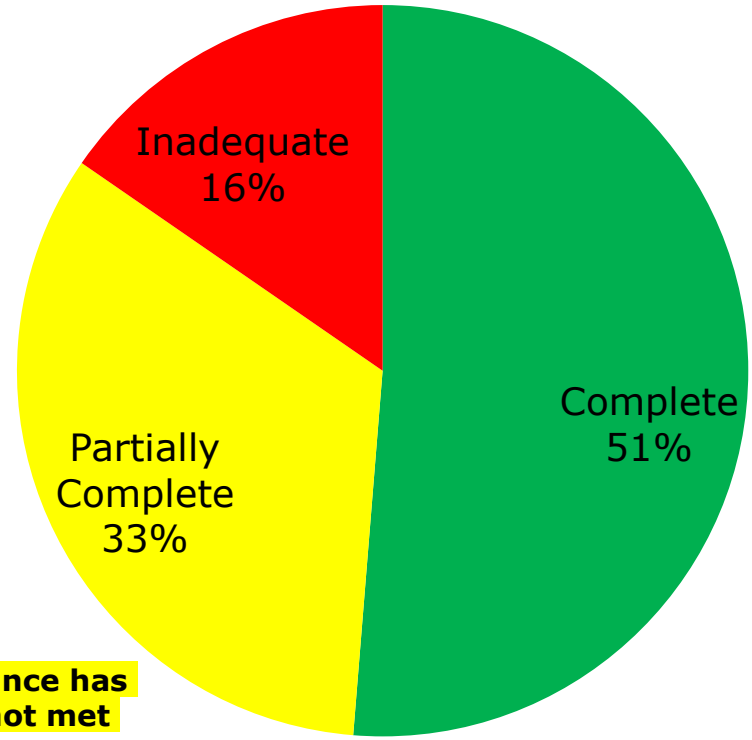
- RA plans must be submitted annually
- RAs must be performed every 3 years
- BIA's must be submitted annually
- Risk Treatment Plans must be updated quarterly
- Agency ISO is certified

Risk Program Compliance Grades



Risk Program Compliance

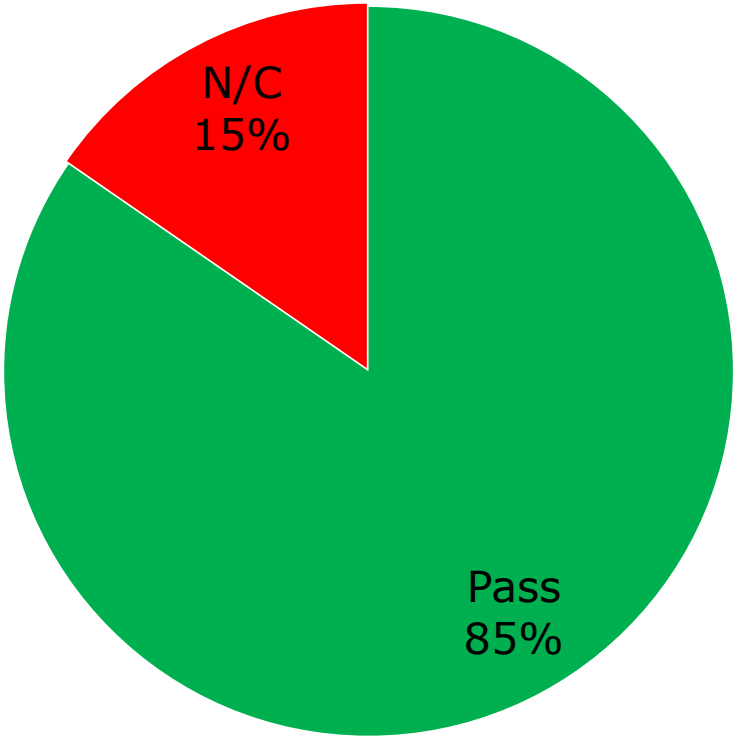
Overall risk program compliance increased by 10 percent



Three year risk assessment obligation compliance has improved; however, most agencies still have not met this obligation.

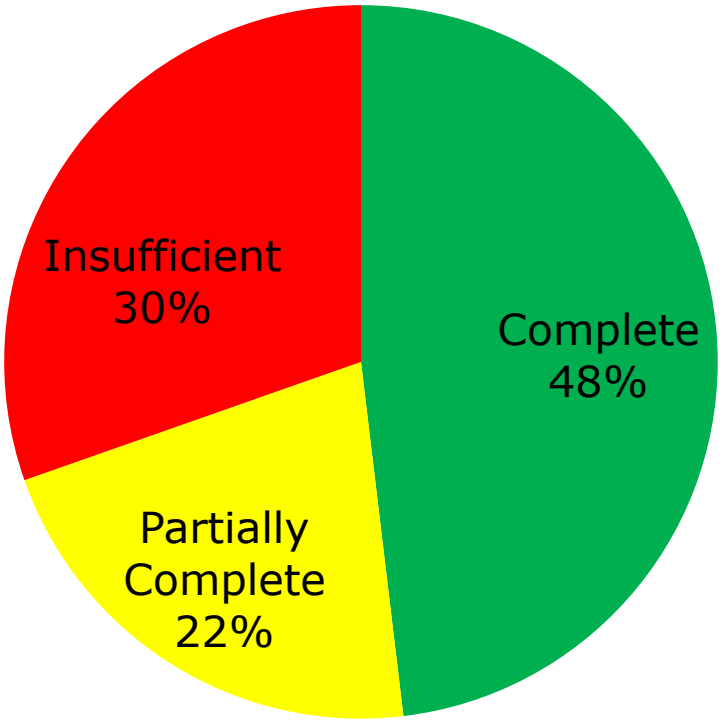
Risk Plan Status

Risk Assessment Plan



Risk Assessment Obligation

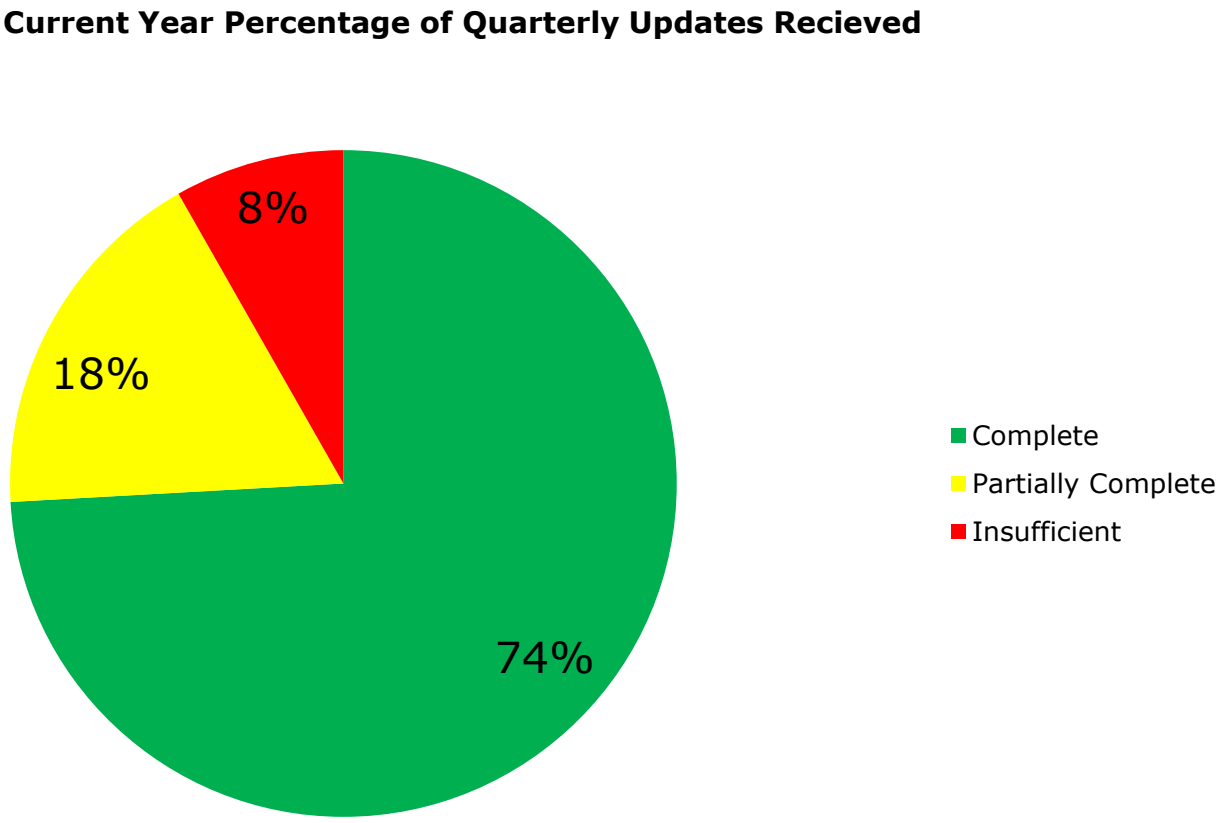
Three Year Risk Assessment Obligation



Three year risk assessment obligation increased by 11 %

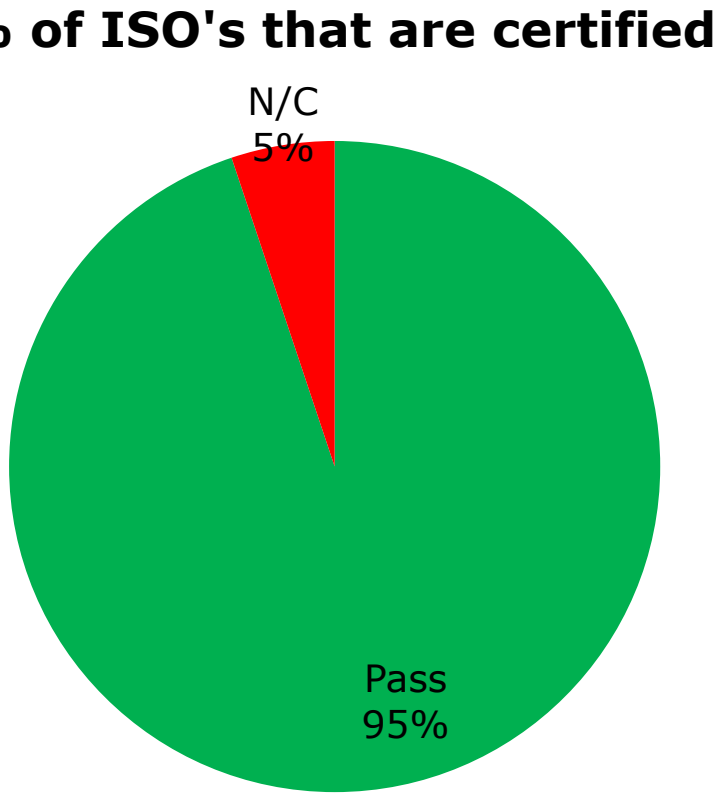
Percentage of Quarterly Updates Received

Quarterly updates received increased by 4 percent

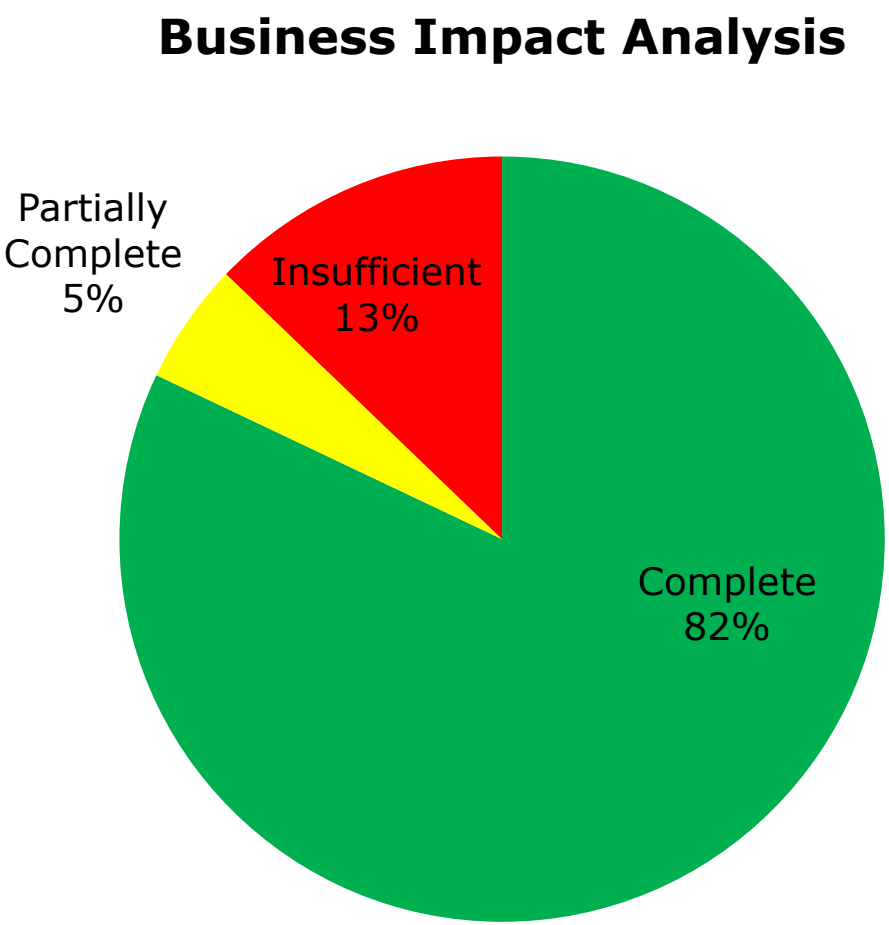


% of ISOs that are Certified

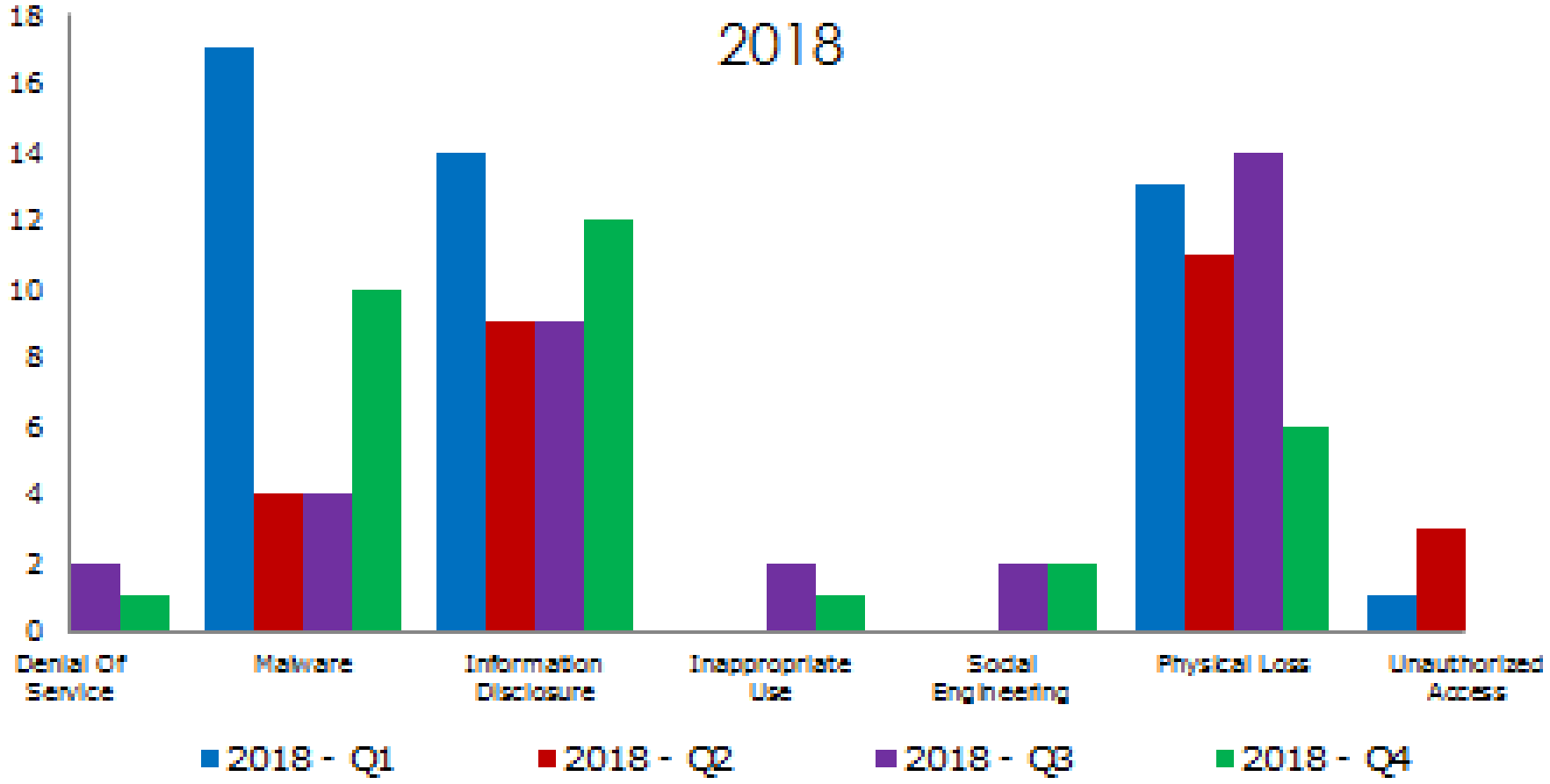
The % of ISO's that are certified increased by 7 percent



BIA Summary


Business Impact Analysis
Partially Complete 5%
Insufficient 13%
Complete 82%

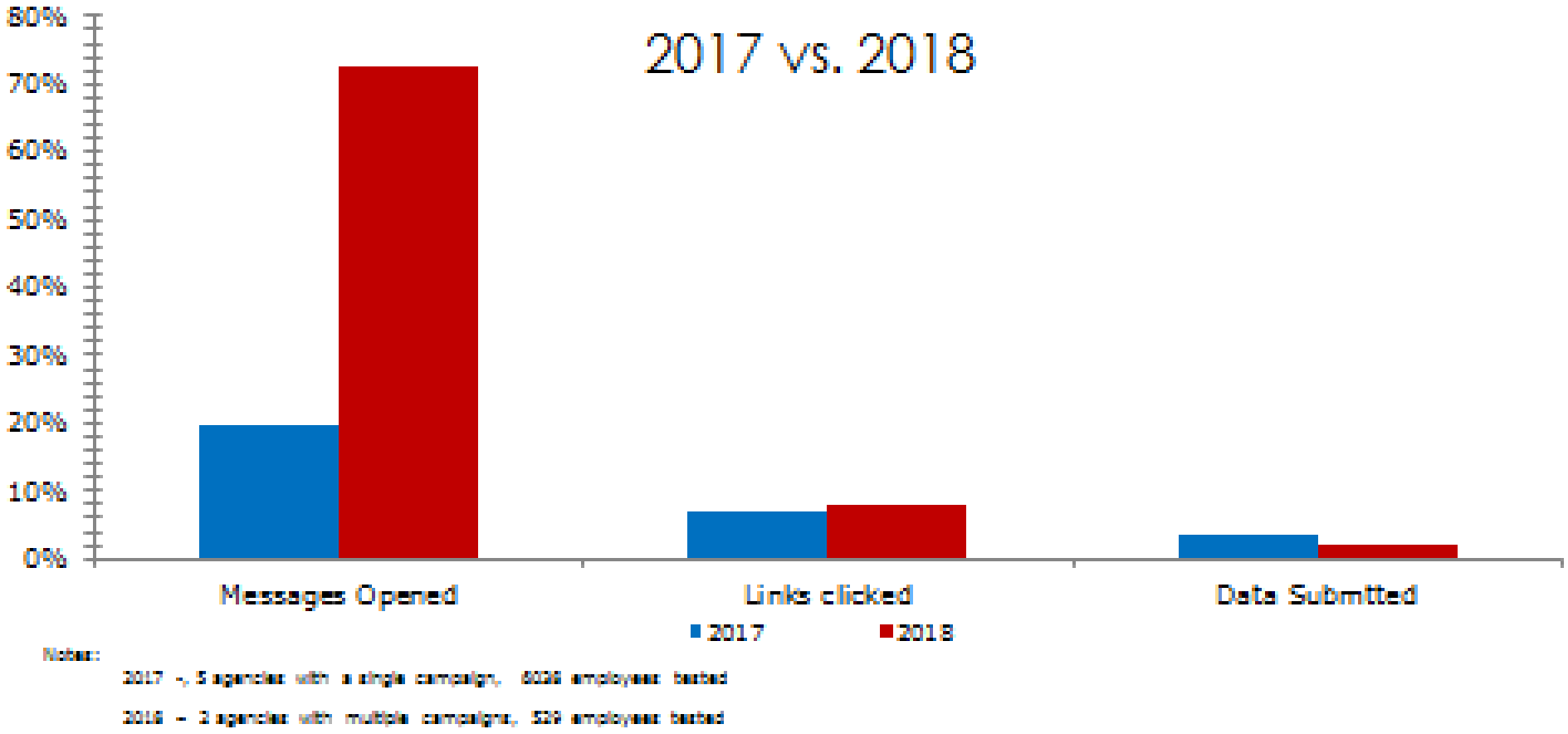
Cyber Security Incident Trends by Category



Security Awareness Training

- **Security awareness training is key to protecting COV employees, systems and data from cyberattacks.** As the attack landscape is constantly changing, the primary point of defense remains the same – the employee. While technical controls can be put in place to protect the environment, the only effective approach is employee training.

CoVA Simulated Phishing Results

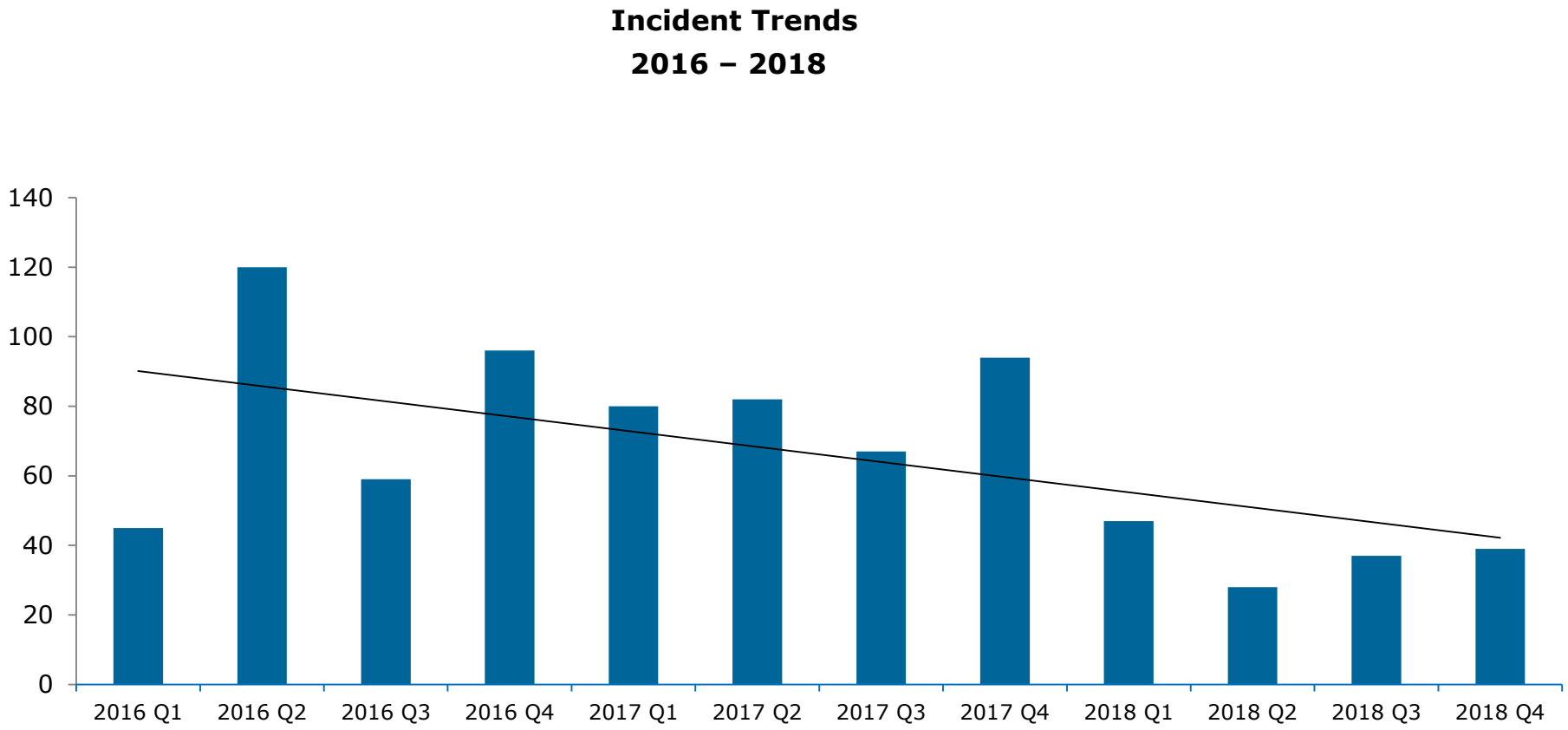


Notes:

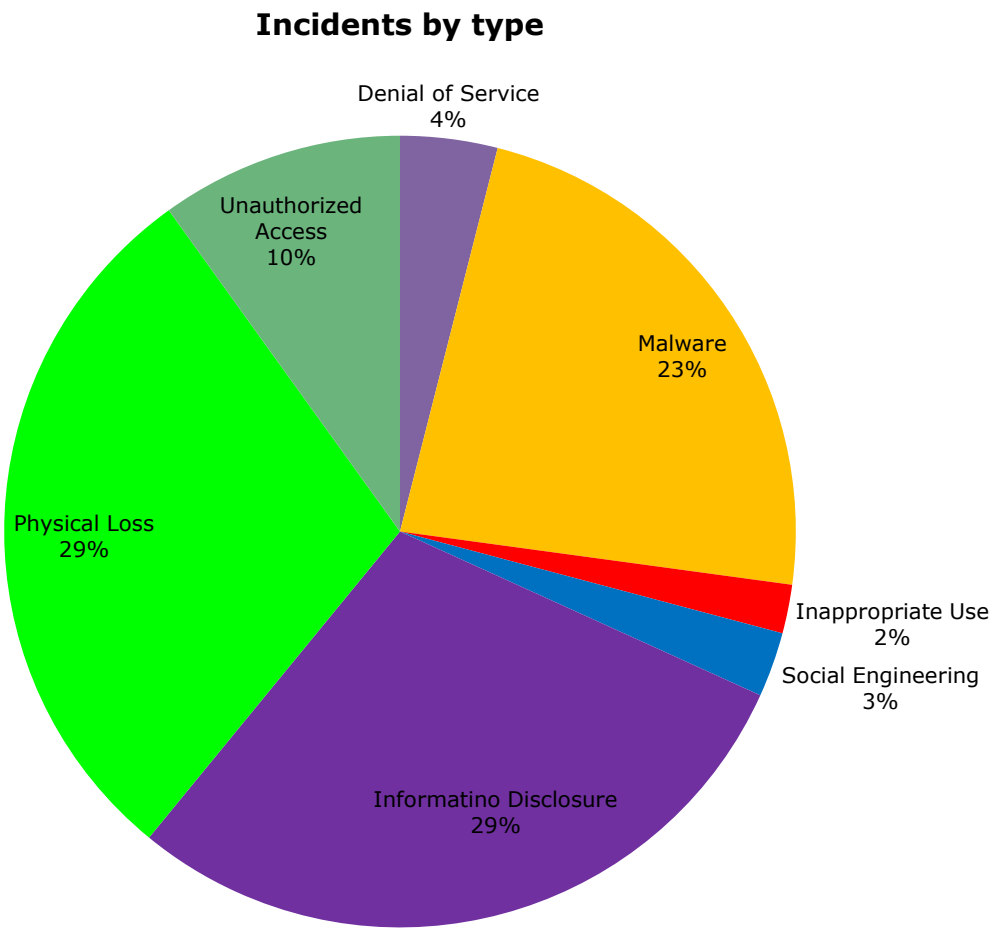
2017 – 5 agencies with a single campaign, 6038 employees tested

2018 – 2 agencies with multiple campaigns, 529 employees tested

Incident Trends 2016-2018

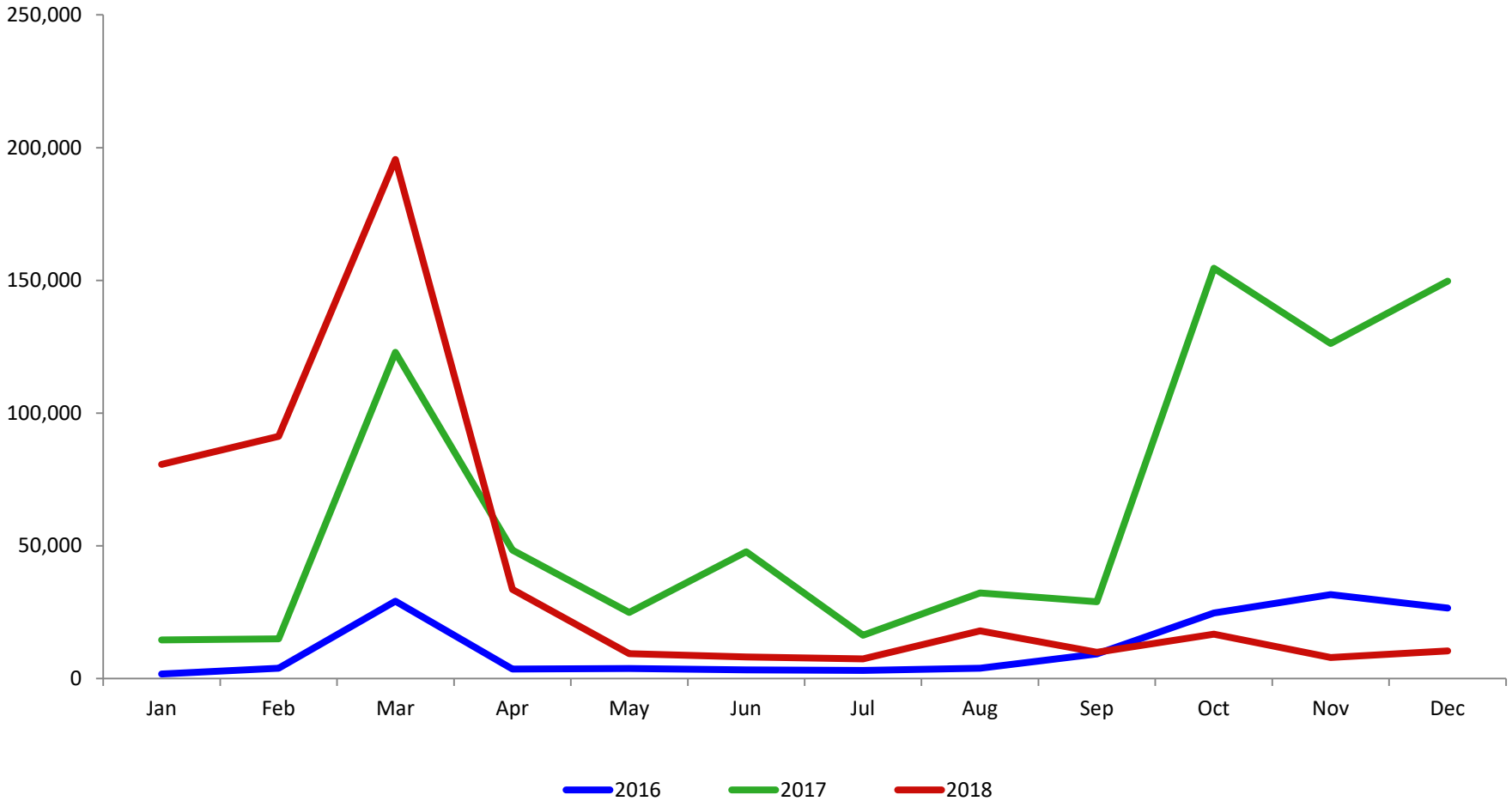


Incidents by Type

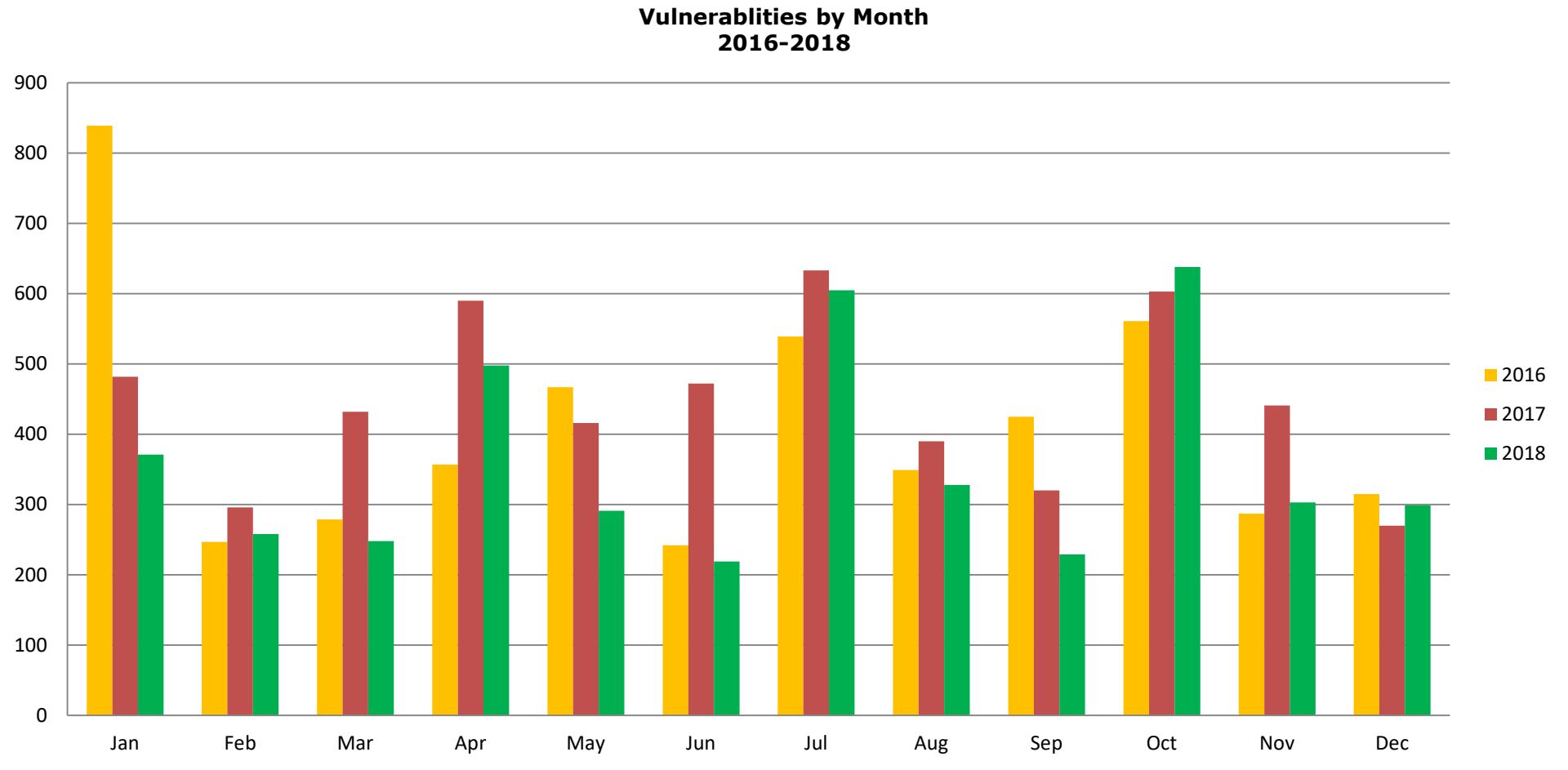


Total incidents for COV: 151
Estimated cleanup costs: $90,600

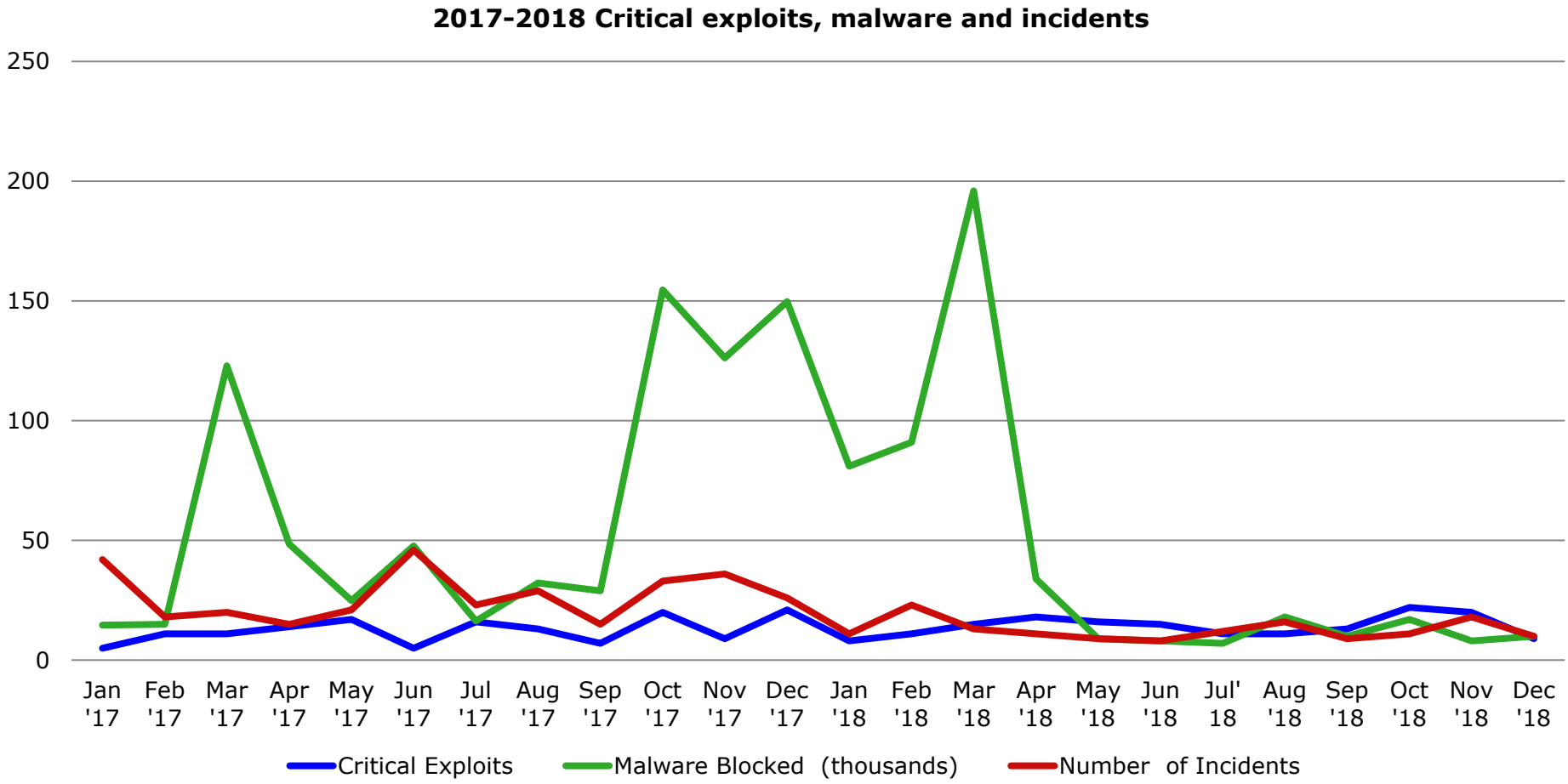
Malware Blocked 2016 - 2018



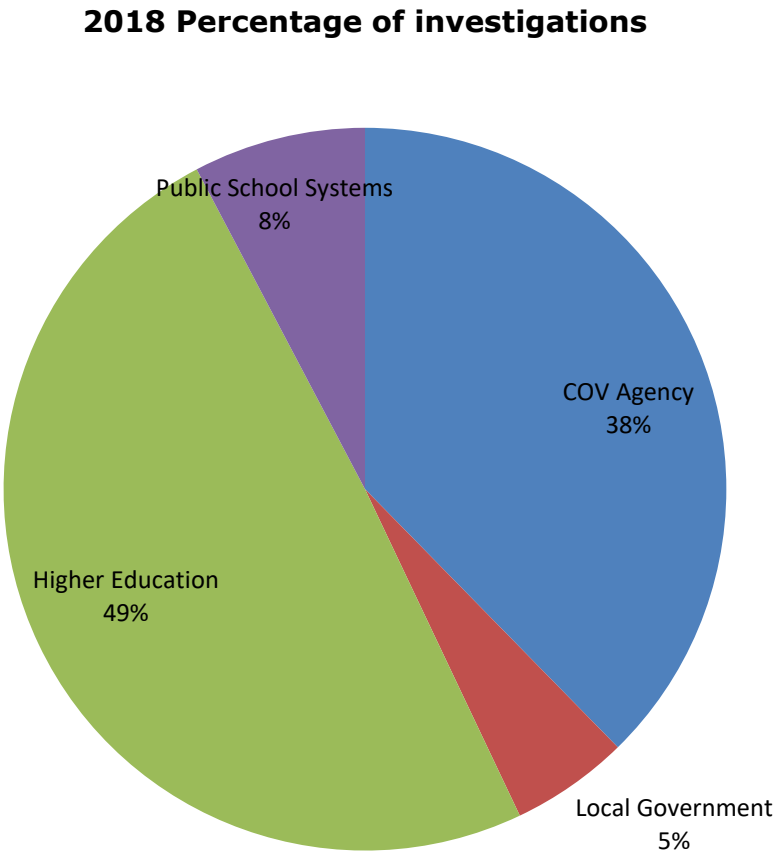
Vulnerabilties by Month 2016 – 2018



Critical Exploits



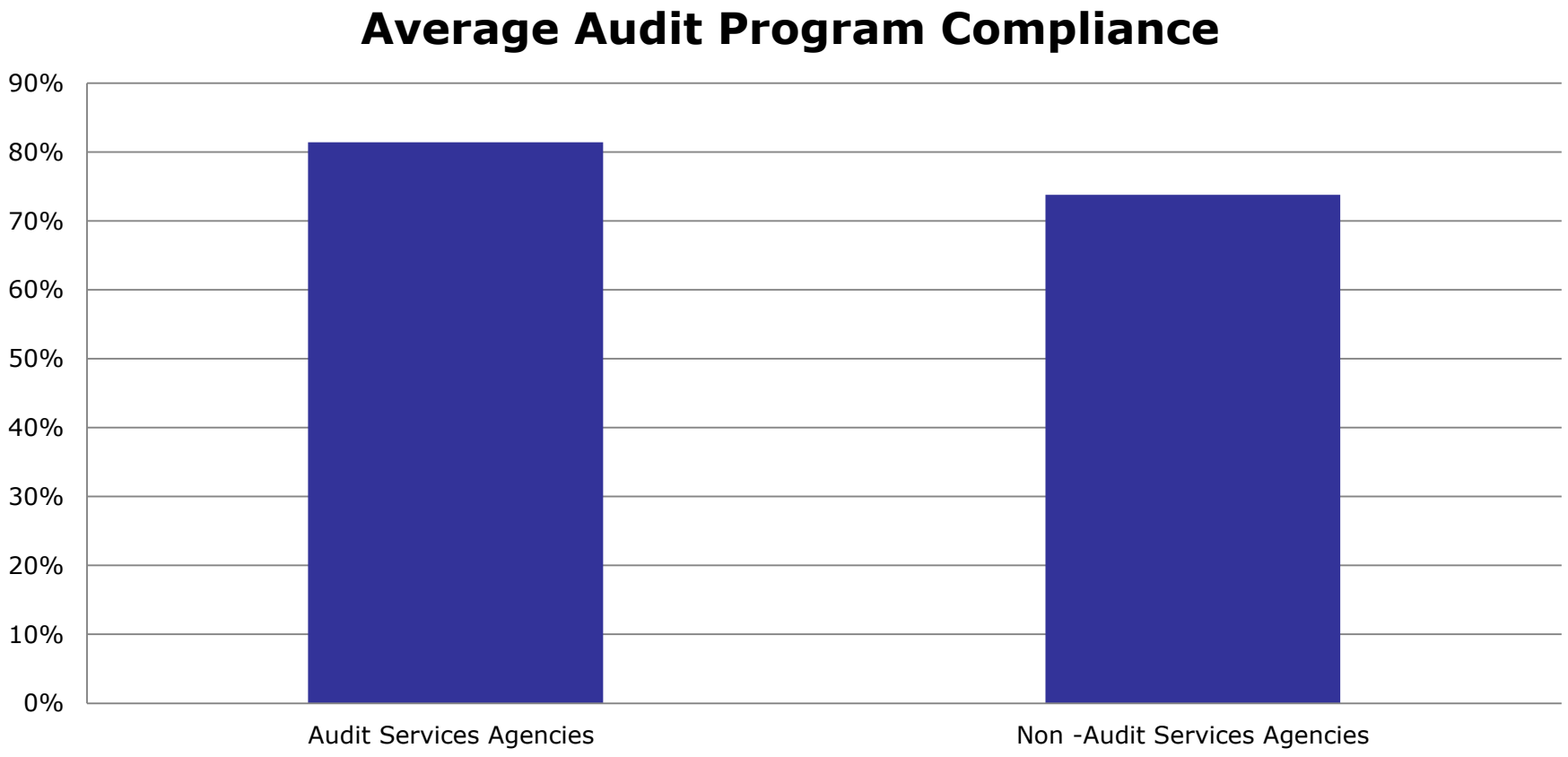
2018 Percentage of Investigations



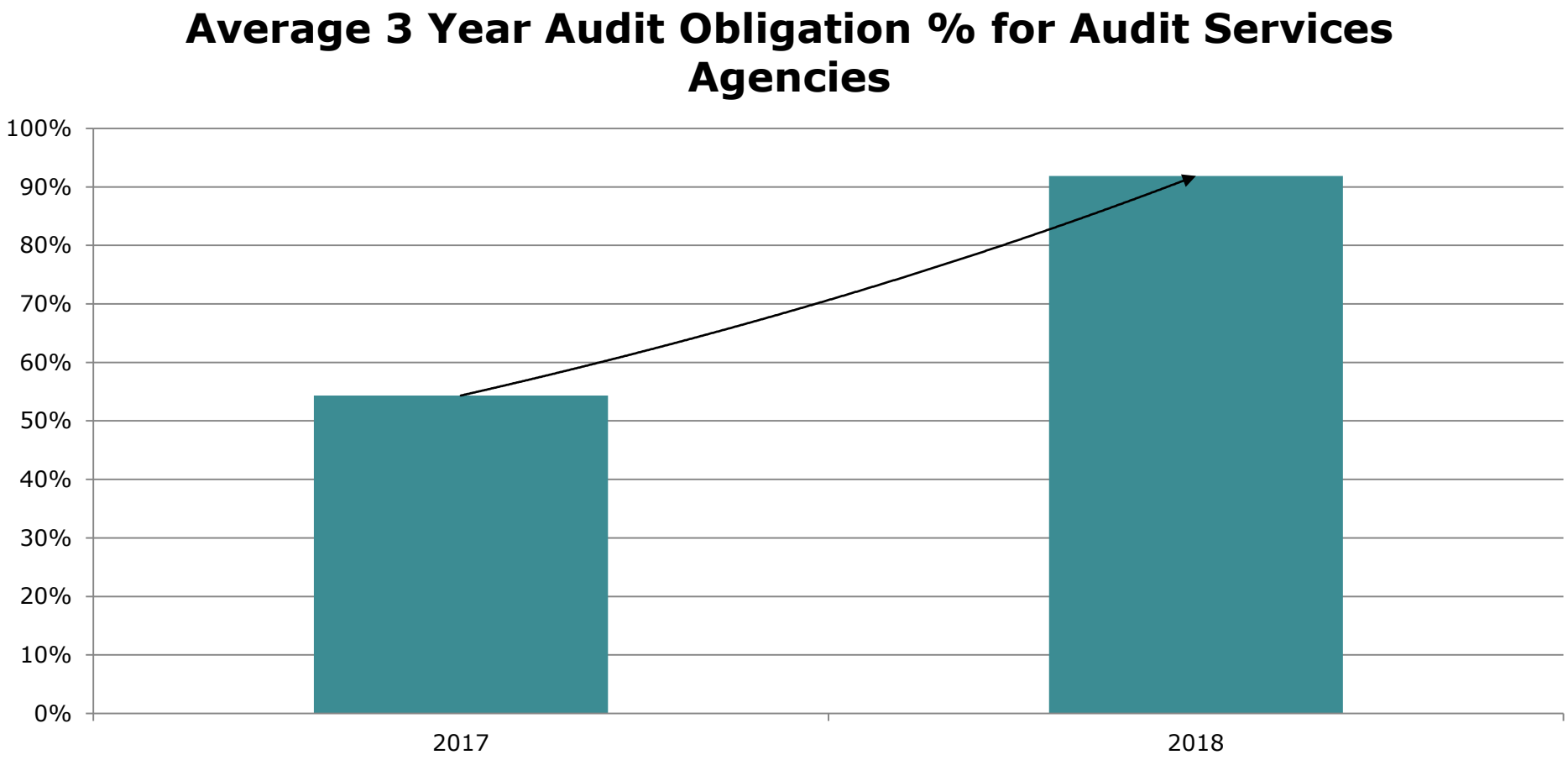
Security Investigations by Category

	Higher education	Local government	Public school systems	COV agencies
Accounts compromised	39%	3%	56%	2%
Malware infections	37%	0%	1%	61%
Cyberattacks	67%	8%	13%	13%
Software vulnerabilities	38%	12%	23%	27%
***Potential loss associated with records exposed**	$186,086	$38,038	$93,790	$57,365

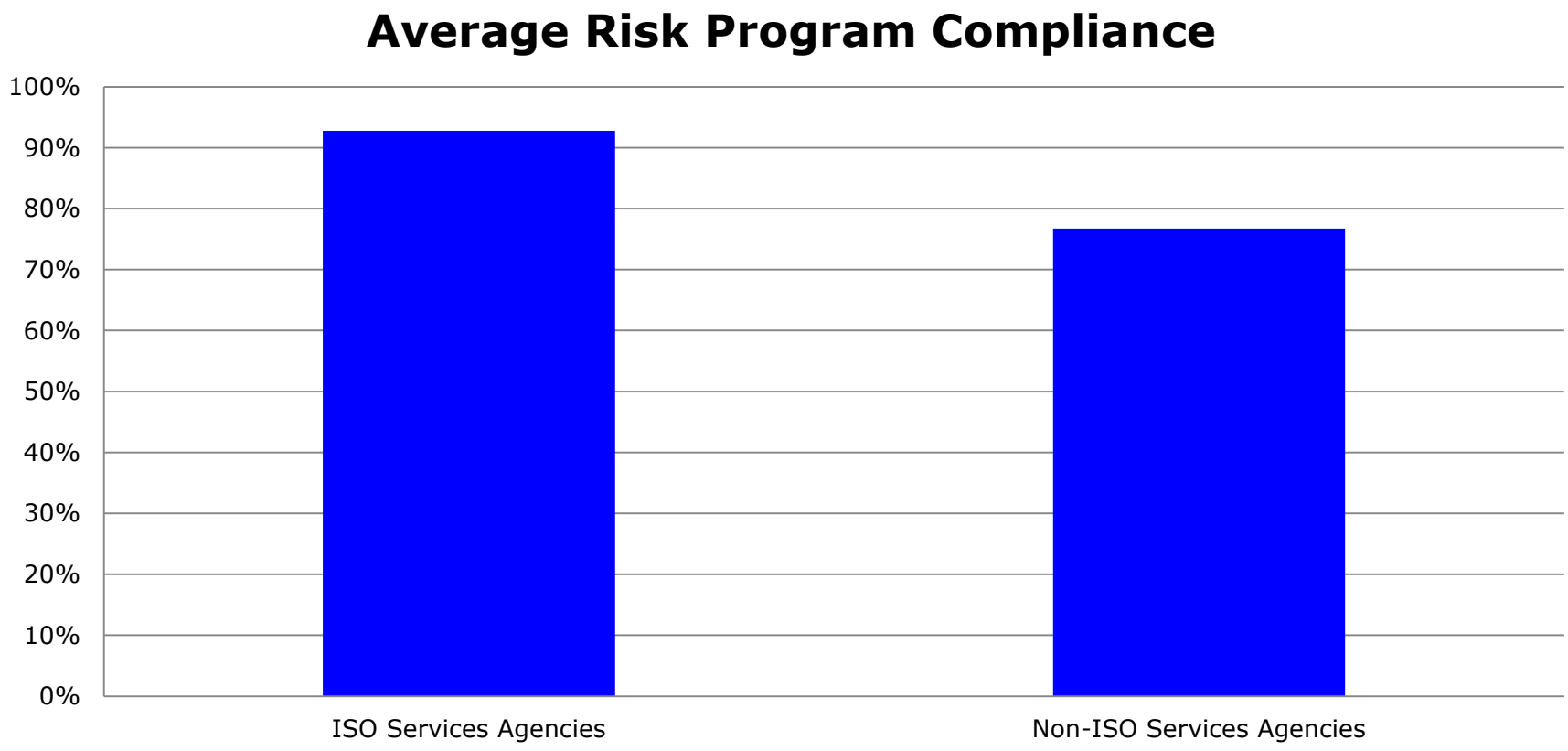
Centralized Services - Audit



Centralized Services - Audit



Centralized Services - ISO



NCSR

Commonwealth agencies continue to participate in the Nationwide Cyber Security Review (NCSR), a cyber network security assessment designed to measure security gaps and capabilities.

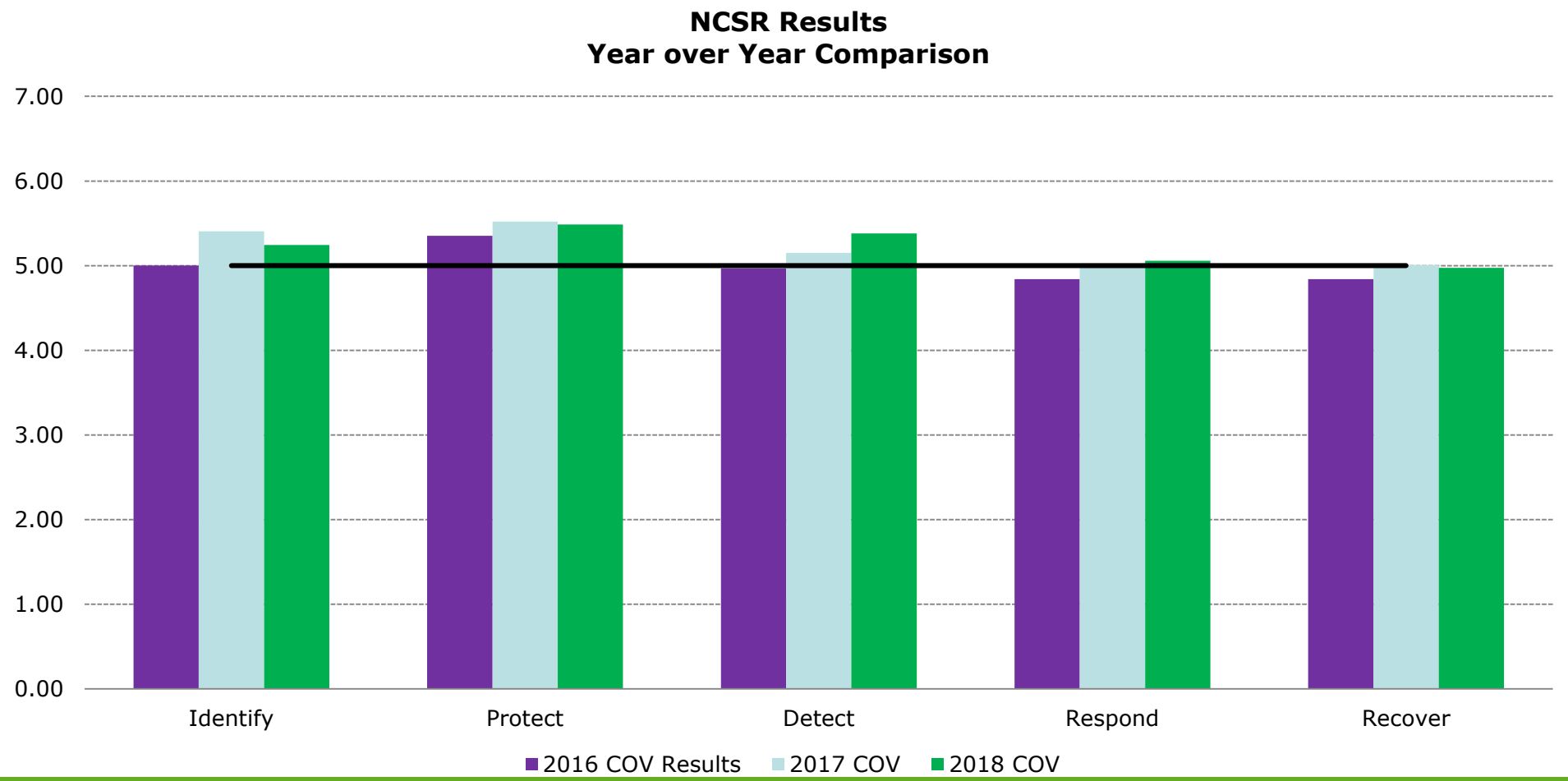
NCSR

The NCSR questions are built on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) core.

The five main functions of the NCSR are: Identify, Protect, Detect, Respond and Recover. Each function is subdivided into categories and then further into subcategories.

Score	Maturity Level *The recommended minimum maturity level is set at a score of 5 and higher*	
7	**Optimized:**	Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	**Tested and Verified:**	Your organization has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	**Implementation in Process:**	Your organization has formally documented policies, standards, and procedures and are in the process of implementation.
5	**Risk Formally Accepted:**	Your organization has chosen not to implement based on a risk assessment.
4	**Partially Documented Standards and/or Procedures:**	Your organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy.
3	**Documented Policy:**	Your organization has a formal policy in place.
2	**Informally Performed:**	Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.
1	**Not Performed:**	Activities, processes and technologies are not in place to achieve the referenced objective.

NCSR Survey Results



2nd Annual Report Requirement

In 2.2-2009 Additional duties of the CIO relating to security of government information.

C. …the CIO shall conduct an annual comprehensive review of cybersecurity policies of every executive branch agency, with a particular focus on any breaches in information technology that occurred in the reviewable year and any steps taken by agencies to strengthen cybersecurity measures.

2nd Annual Report Requirement

Upon completion of the annual review, the CIO shall issue a report of his findings to the Chairmen of the House Committee on Appropriations and the Senate Committee on Finance.

Such report shall not contain technical information deemed by the CIO to be security sensitive or information that would expose security vulnerabilities.

2nd Annual Report Requirement

Criteria:

- Analyze Archer for all Audit and Risk Findings that relate to IT security policy deficiencies.
- Review Archer and other soruces for all security incidents that might be attributable to deficient policies or inadequate training.
- Review each agency's NCSR survey results.

- Expect that report in late summer 2019

Questions?

You may also send any questions to :
CommonwealthSecurity@VITA.Virginia.Gov