



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

April 1, 2015



ISOAG April 1, 2015 Agenda

- | | |
|---|---------------------------------------|
| I. Welcome & Opening Remarks | Michael Watson, VITA |
| II. Applying Risk Management From the Enterprise Through Cyber Security for Focus and Allocation of Resources | Peter Allor, IBM |
| III. Preview - Draft 2014 Annual Report | Mark Martens, VITA |
| IV. Upcoming Events | Bob Baskette/Michael Watson, VITA |
| V. Partner/Operation Update | Bob Baskette, VITA, Michael Clark, NG |



Welcome and Opening Remarks

Michael Watson

April 1, 2015



Virginia Information Technologies Agency

Peter Allor, IBM

“Applying Risk Management From the Enterprise Through Cyber Security for Focus and Allocation of Resources”

April 1, 2015

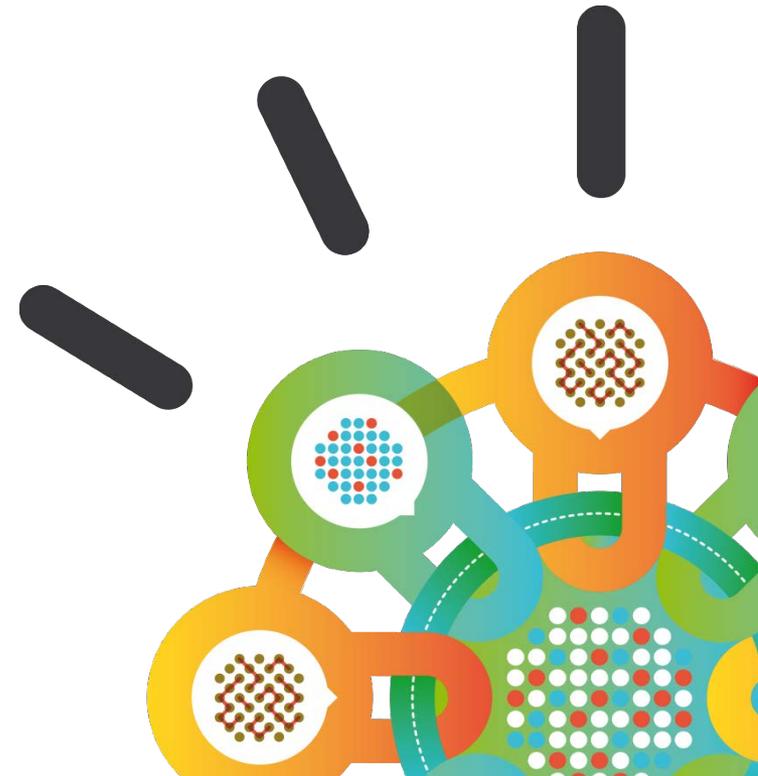
Security Intelligence.
Think Integrated.

Security Threats, Frameworks, and Mitigation Efforts

How Can You Lower Your Risk?

Peter Allor
Security Strategist

April 2015



83% of CISOs say that the challenge posed by external threats has increased in the last three years

Near Daily Leaks of Sensitive Data

40% increase in reported data breaches and incidents

Relentless Use of Multiple Methods

800,000,000+ records were leaked, while the future shows no sign of change

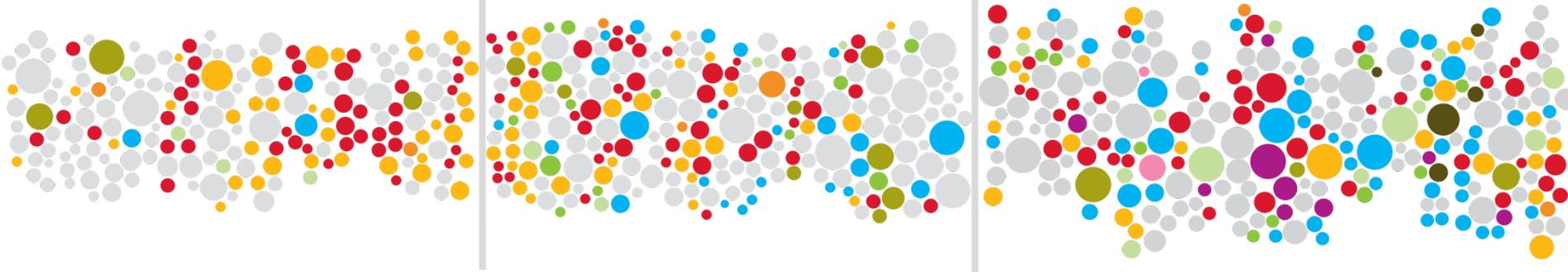
“Insane” Amounts of Records Breached

42% of CISOs claim the risk from external threats increased dramatically from prior years.

2012

2013

2014



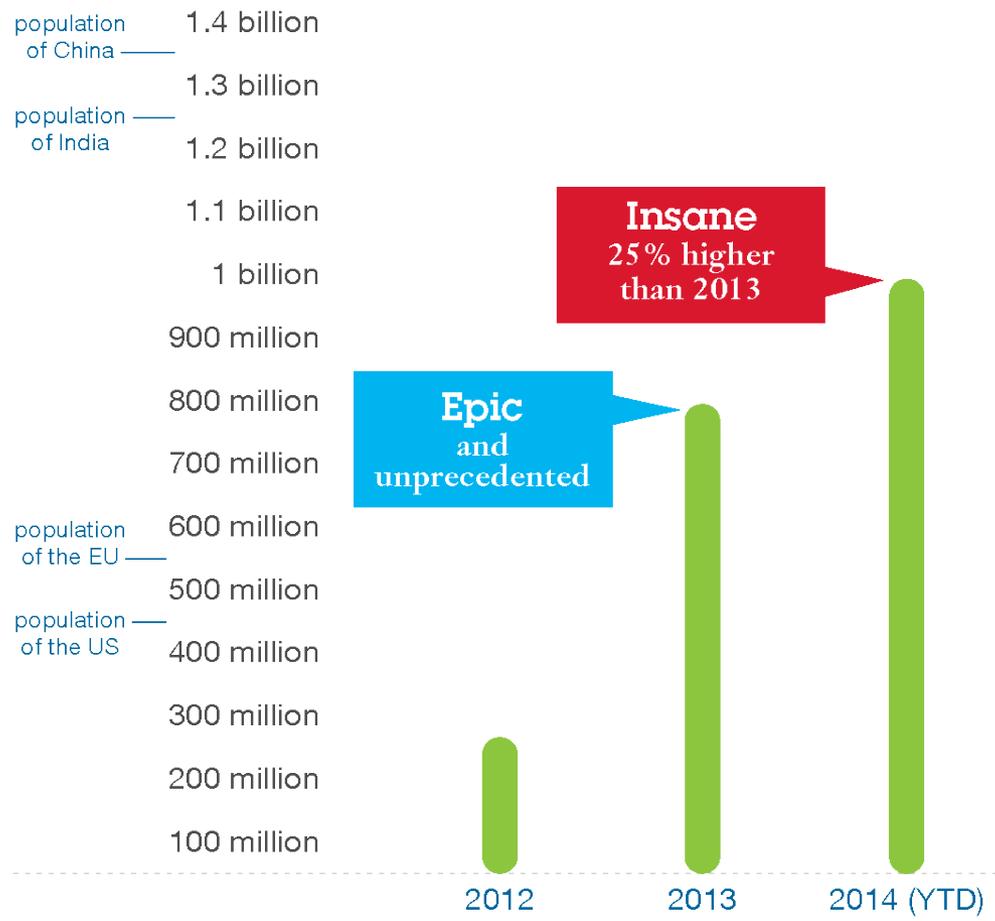
Size of circle estimates relative impact of incident in terms of cost to business.

A historical look at security incidents by attack type, time and impact, 2012 through 2014

Based on pure volume, the total number of records breached in 2014 was nearly 25 percent higher than in 2013

Total records leaked by year

compared to estimated population sizes



New technologies introduce new risks...

70%



of security executives have **cloud and mobile concerns**

2013 IBM CISO Survey



614%

Mobile malware growth
in just one year

2012-2013 Juniper Mobile Threat Report

...and traditional security practices are unsustainable

85



security tools from

45



vendors

IBM client example

83%



of enterprises have difficulty finding the **security skills** they need

2012 ESG Research

CISOs face a shortage of skills, lack of metrics and strategy



49% 
of IT executives have **no measure of security effectiveness**

2012 Forrester Research Study

31% 
of IT professionals have **no risk strategy**

2013 Global Reputational Risk & IT Study, IBM

83% 
of enterprises have difficulty finding the **security skills** they need

2012 ESG Research

Highly regulated industries have the highest per-record data breach costs



\$359
Healthcare



\$294
Education



\$227
Pharmaceutical



\$206
Financial



\$155
Consumer



\$141
Energy

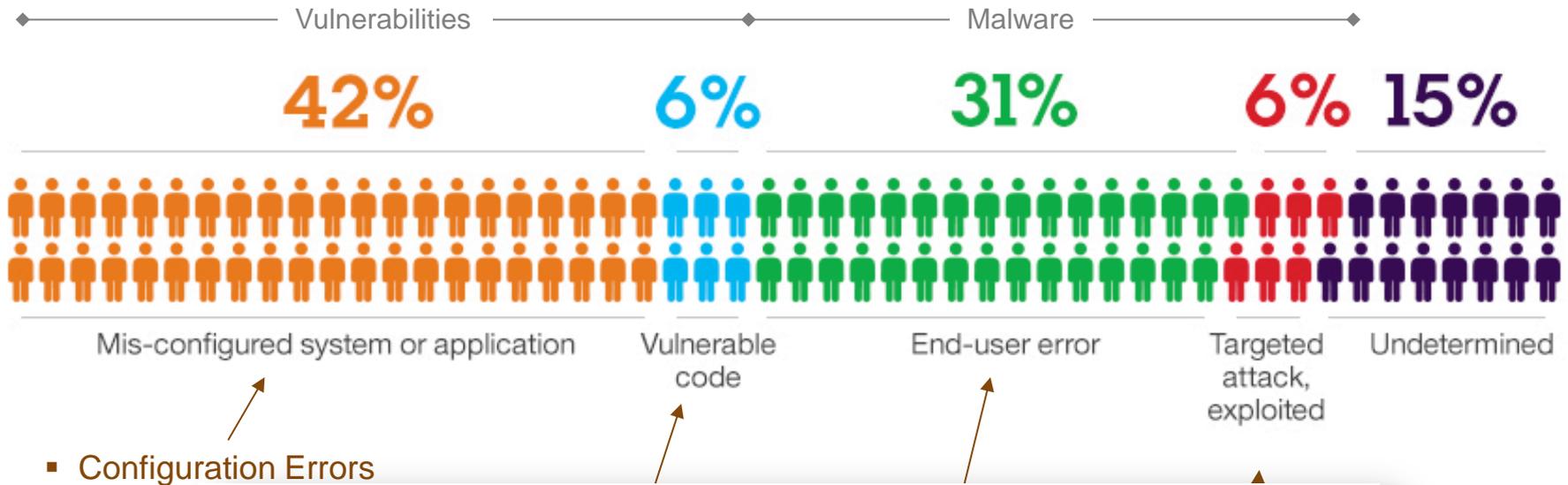


\$122
Hospitality



\$105
Retail

Why do Breaches Happen?



- Configuration Errors
- “Weak” c
- Easy pa



**The Human Factor:
How Breaches Occur**

Many elements can contribute to the vulnerability of your organization, however none is more prevalent than the human factor, **which accounts for approximately 80%.**

- Phishing Emails
- Watering Hole attacks

Security leaders are more accountable than ever before



CEO	CFO/COO	CIO	CHRO	CMO
Loss of market share and reputation Legal exposure	Audit failure Fines and criminal charges Financial loss	Loss of data confidentiality, integrity and/or availability	Violation of employee privacy Violation of customer privacy	Loss of customer trust Loss of brand reputation

Your board and CEO demand a strategy

Questions CISO Want to be Able to Answer...

Establishing Baseline

Identify what needs to be defended or observed as well as formulate a risk profile to detect abnormalities

- Who are the attractive targets within my enterprise?
- Which applications and what data do we need to defend due to their sensitivity?
- What is the normal behavior profile for users, assets, and applications?

Sophisticated Attacks

Gain awareness of a motivated/ incentivized attacker attempting to hide/ disguise the attack as innocuous interactions, potentially over a long period of time

- Which assets within my organization are already compromised or are vulnerable?
- Which external domains may be the source of attacks?
- Are there any low profile network traffic elements that might signal an ongoing or imminent attack?

Qualify Insider Threats

Identify or warn of users within the organization's network who may be inclined to perform actions that are detrimental to the organization's operations

- What data is being leaked or lost and by whom?
- Who internally has the motivation and skills to compromise the cyber operations of the company?
- Who is exhibiting abnormal usage behavior?

Predict Hacktivism

Alert to a possible attack from groups or entities that sympathize with causes that are contrary to the interests

- Which controversial issues may trigger a negative sentiment about the organization triggering an increased risk of attack?
- How to identify and monitor intentions of entities antagonistic to the organization's business practices?
- How does publicity of the company in the media impact risk?

Counter Cyber Attacks

Inform of an impending or on-going attack by criminal enterprises or government funded or government sponsored groups

- Which geographical region may be the origin of an attack?
- Which hacking tools may be used and who is gaining access to them?
- Are their symptoms of an attack underway or being planned manifesting themselves as support issues?

Mitigate Fraud

Surface new or existing fraud methods that may compromise its compliance with regulations or cause significant losses to its financial operations

- How can the organization identify a fraudulent activity?
- Which users have compromised identities that may lead to fraudulent activity?
- Can well known fraud attempts have patterns can either be detected or even anticipated?

The 2014 U.S. State of Cybercrime Survey

The survey identified eight common deficiencies where spending and efforts lag:

1. **Most organizations do not take a strategic approach to cybersecurity spending**
2. Organizations do not assess security capabilities of third-party providers
3. Supply chain risks are not understood or adequately assessed
4. Security for mobile devices is inadequate and has elevated risks
5. Cyber risks are not sufficiently assessed
6. Organizations do not collaborate to share intelligence on threats and responses
7. Insider threats are not sufficiently addressed
8. Employee training and awareness is very effective at deterring and responding to incidents, yet it is lacking at most organizations

<http://www.pwc.com/us/en/increasing-it-effectiveness/publications/2014-us-state-of-cybercrime.jhtml>

Co-sponsored by **CSO magazine**, **CERT Division of the Software Engineering Institute at Carnegie Mellon University**, **PwC**, and **the US Secret Service**, March-April 2014



Executive Order 13636: Improving Critical Infrastructure Cybersecurity

“It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties”

*President Barack Obama
Executive Order 13636, Feb. 12, 2013*



- The National Institute of Standards and Technology (NIST) was directed to work with stakeholders to develop a [voluntary framework for reducing cyber risks to critical infrastructure](#)
- Version 1.0 of the framework was released on Feb. 12, 2014, along with a [roadmap for future work](#)

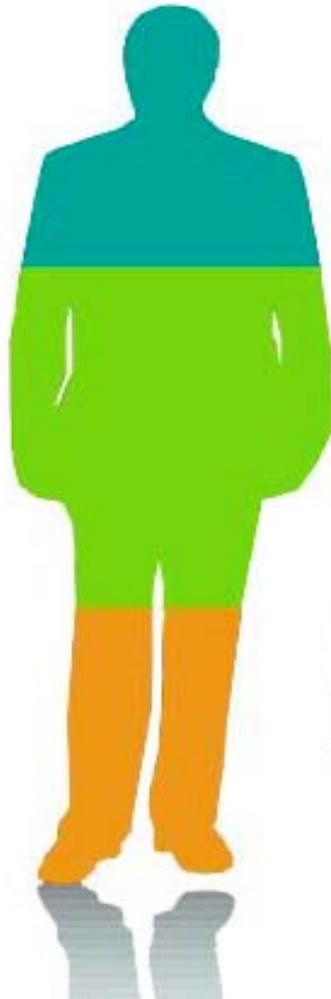
**A new approach
to security
is needed**



IBM CISO Assessment – 2012

Frameworks rely on the CISO having Stakeholder Participation

And their roles are evolving with growing authority, accountability and impact across the enterprise.



Influencers

Confident and prepared, influence the business strategically

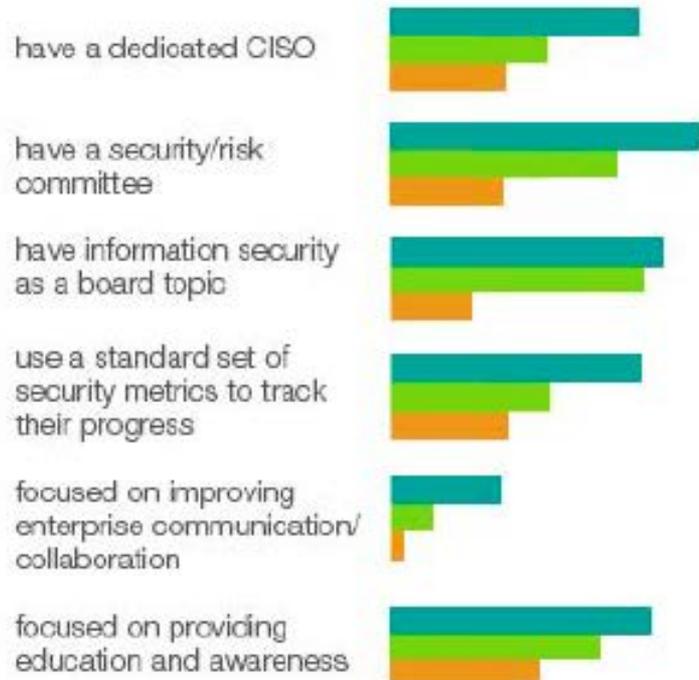
Protectors

Less confident, prioritize security strategically but lack necessary structural elements

Responders

Least confident, focus largely on protection and compliance

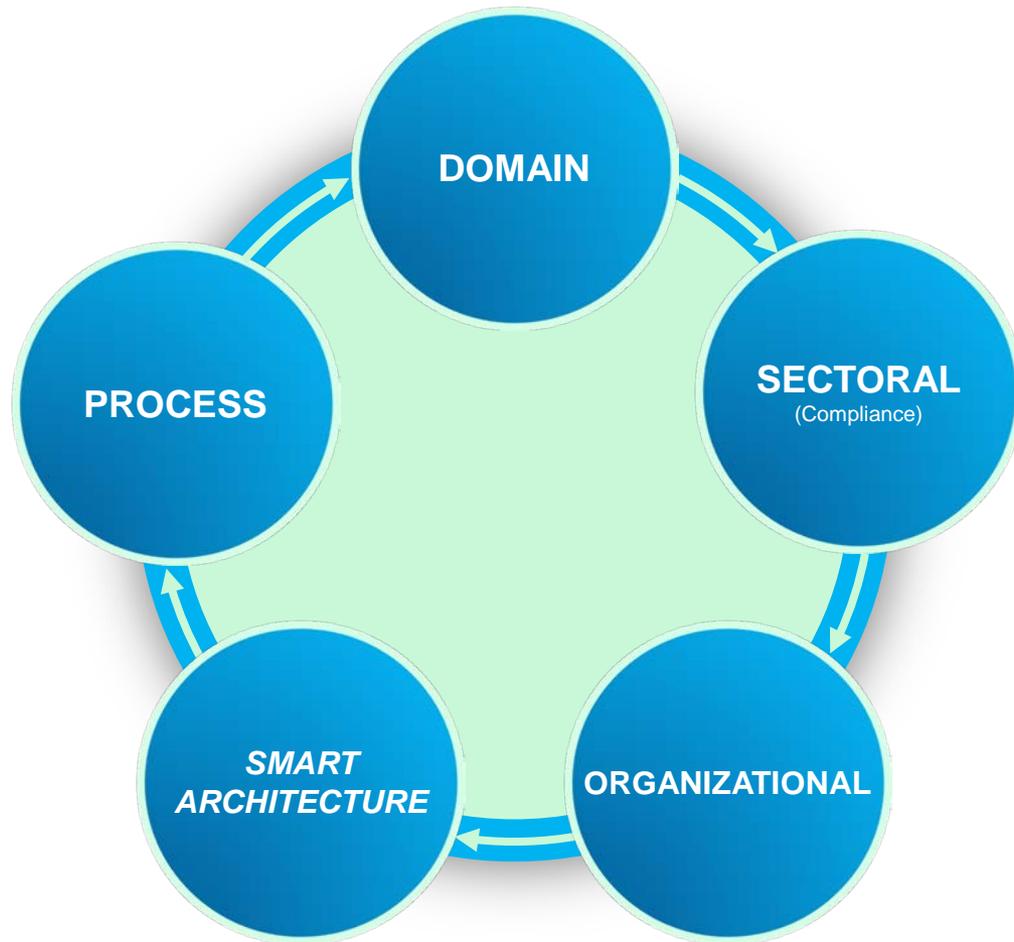
How they differ



Solving security Frameworks



The Five Types of Security Risk Frameworks

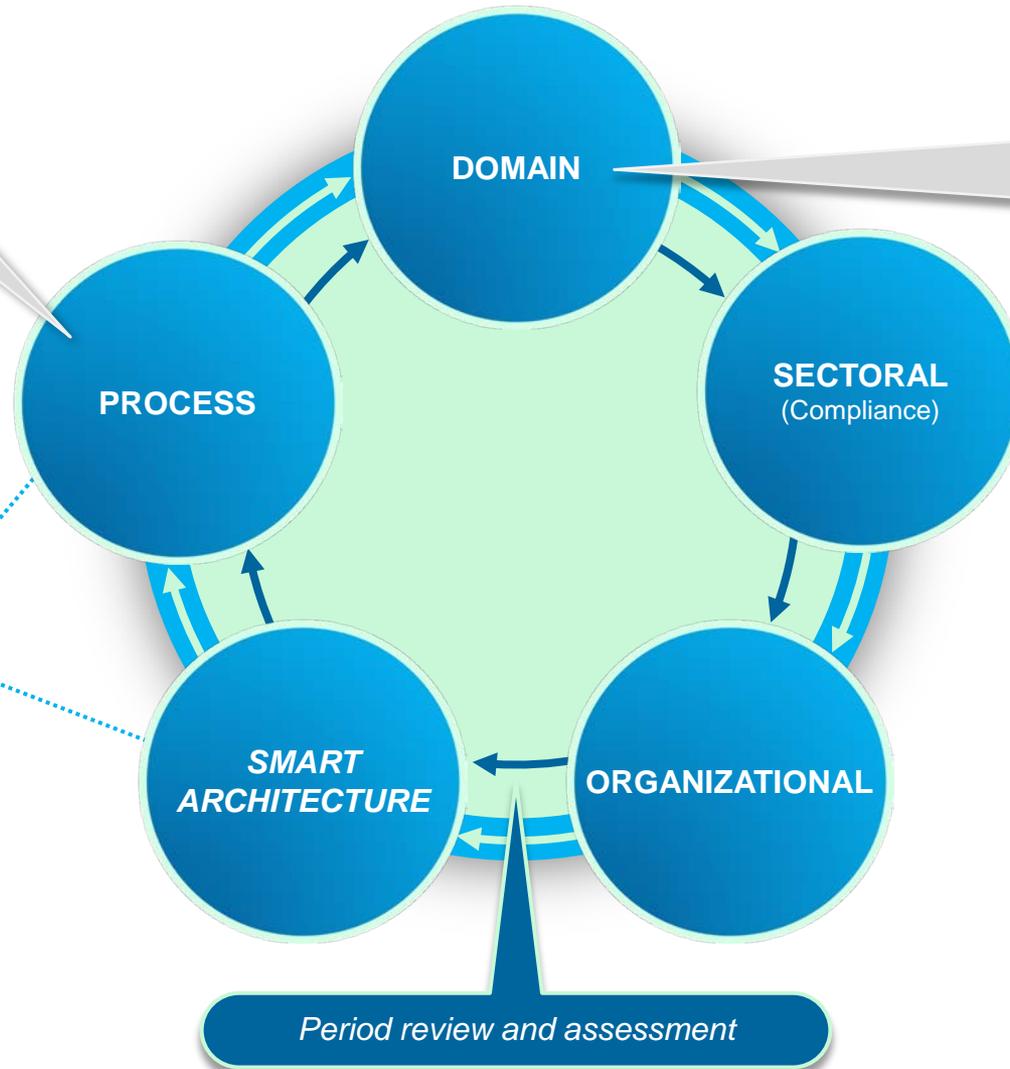


Security Risk Framework Maturity Cycle

NIST Security Framework



No formal strategy



IBM Security Framework



Process Based

Incident response process focus

- Identify
- Prevent
- Detect
- Respond
- Recover



- NIST Cybersecurity Framework
- NIST Risk Management Framework

Continuous diagnostics and mitigation or continuous monitoring

- Phase 1 - Endpoint integrity
- Phase 2 - Least privilege and infrastructure integrity
- Phase 3 - Boundary protection and event management



- USG approach to metrics

Lacks an integrated risk management process to the Organizational Approach for setting risk, priorities, resources and securing the enterprise – focus is on tool sets to measure and metric events to prioritize for remediation

NIST Cybersecurity Framework covers five core functions

Identify

- Develop an organizational understanding to manage cyber-security risk to systems, assets, data and capabilities
- Create an understanding of the business context, resources and risks so the organization can focus and prioritize its efforts

Protect

- Develop and implement safeguards to ensure delivery of infrastructure services and to help limit or contain the impact of a cyber-security event

Detect

- Develop and implement activities to identify the occurrence of a cyber-security event

Respond

- Develop and implement activities to take action following detection of a cyber-security event
- Support the ability to contain the impact of an event

Recover

- Develop and implement activities to maintain resilience and to restore capabilities or services impaired due to a cyber-security event
- Support timely recovery to normal operations

NIST Framework introduces implementation tiers (maturity levels)

Tier 1: Partial

- Organizational cybersecurity risk management practices are not formalized, and risk is managed in a reactive ad hoc manner
- Limited awareness of cybersecurity risk
- An organization-wide approach to managing cybersecurity risk has not been established

Tier 2: Risk Informed

- Risk management practices are approved by management but may not be established as organizational-wide policy
- An awareness of cybersecurity risk but an organization-wide approach to managing cybersecurity risk has not been established

Tier 3: Repeatable

- Risk management practices are formally approved and expressed as policy
- An organization-wide approach to manage cybersecurity risk
- Organization understands its dependencies and partners

Tier 4: Adaptive

- Adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities
- Managing cybersecurity risk that uses risk-informed policies, processes, and procedures
- Manages risk to improve cybersecurity before a cybersecurity event occurs

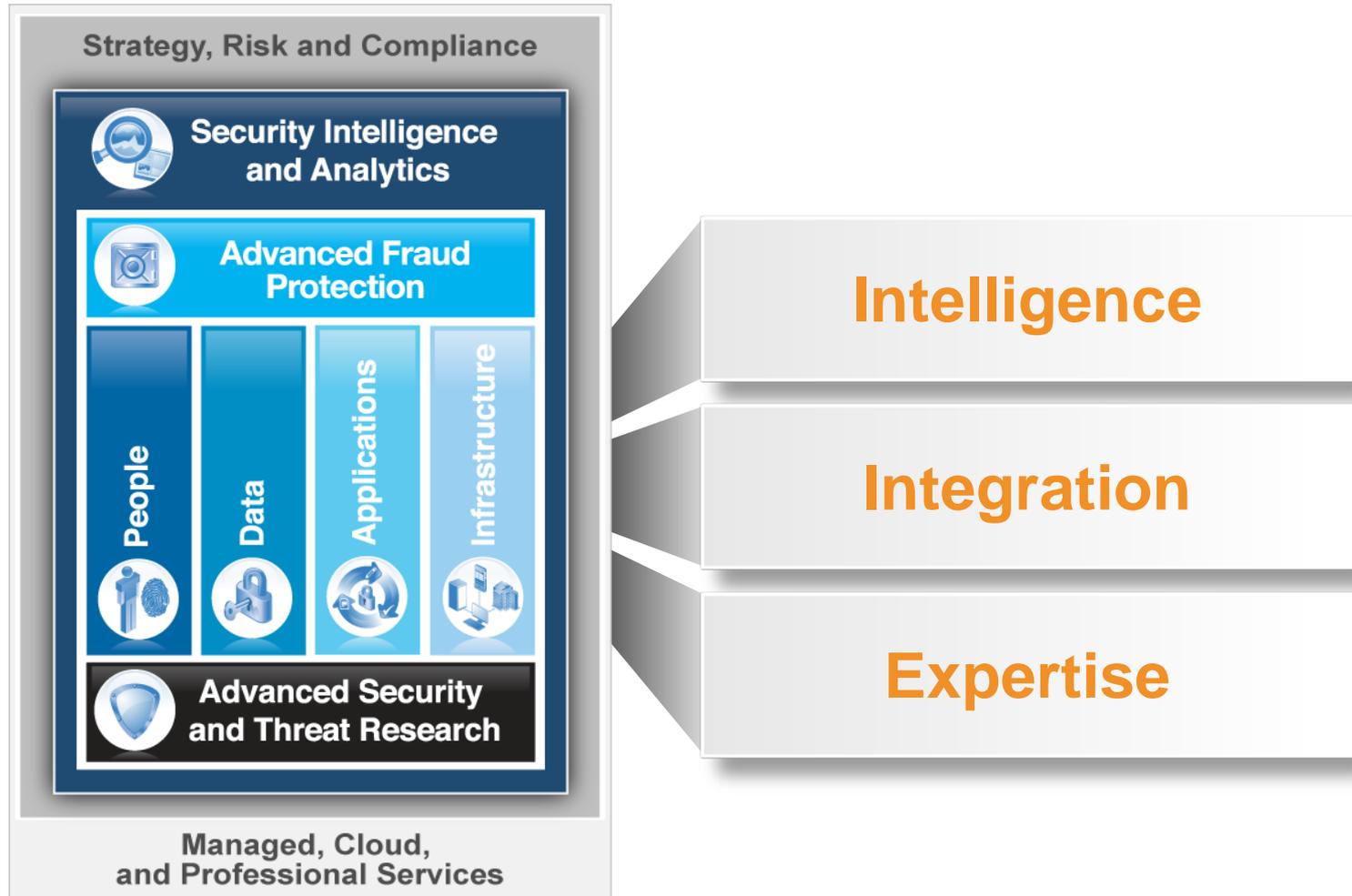
NIST – Framework Profiles

- Calls for a ‘Current’ and a “Target” profile
- Represents the outcomes based on business needs that an organization has selected from its framework(s)
- Can be used to measure current state
- Can support prioritization and measurement of progress toward future state
- Factors in other business needs including cost-effectiveness and innovation
- Can be used to conduct self-assessments and communicate within an organization or between organizations

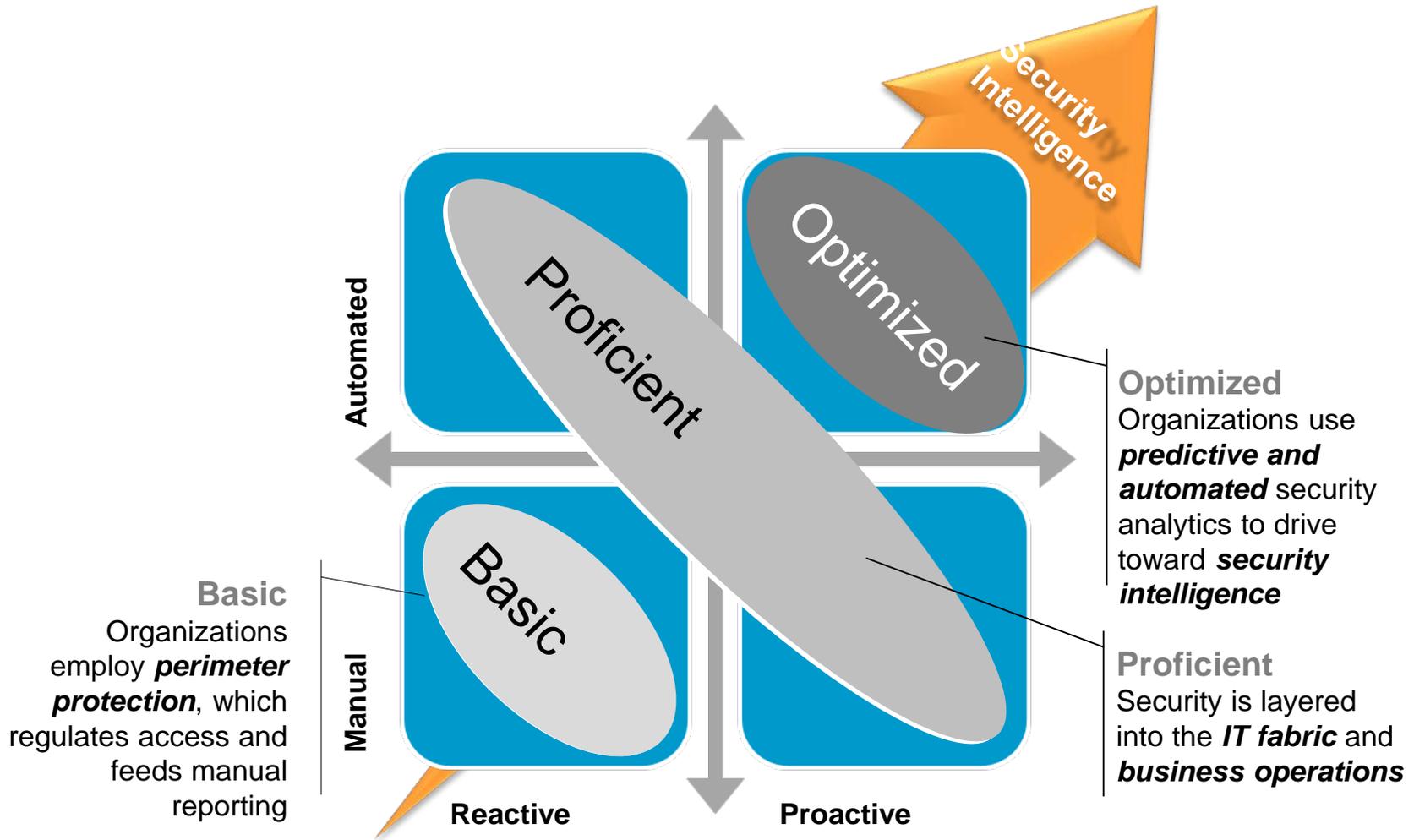
Domain Based: Cobit, ISO Standard based, IBM



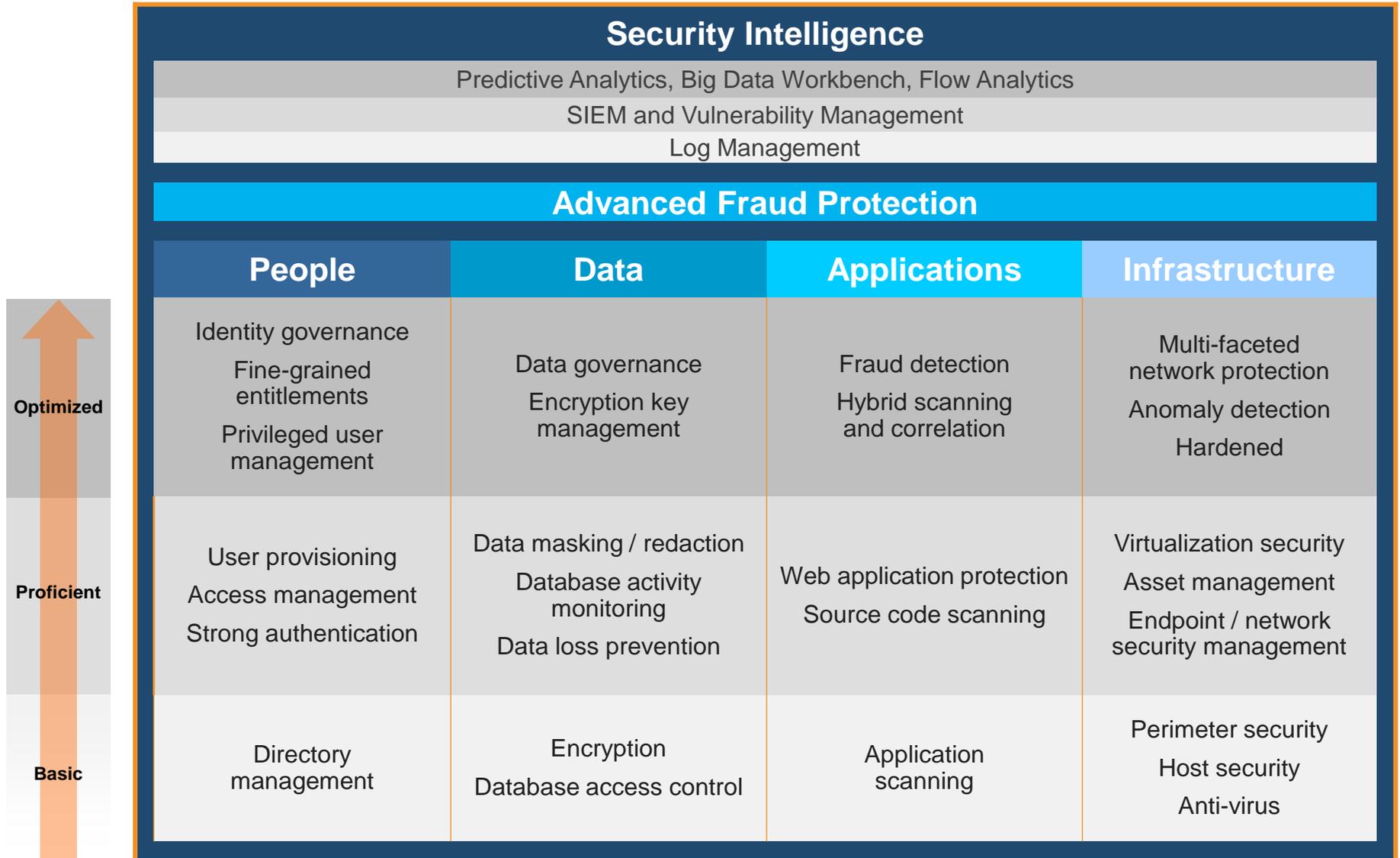
IBM Security: Delivering intelligence, integration and expertise across a comprehensive framework



In this “new normal”, organizations need an intelligent view of their security posture



Reaching security maturity – how to map your way there



Framework Maturity – simplified (Identity and Access focus)

Basic

- Managing secure directories
- Encrypting data
- Scanning applications for vulnerabilities
- Deploying host and perimeter anti-virus security

Proficient

- Controlling user identities and access management
- Monitoring database activity
- Securing web applications
- Scanning source code
- Virtual infrastructures, endpoints and networks

Optimized

- Governing identities and managing privileged users
- Managing encryption keys
- Detecting fraud
- Performing hybrid scanning and correlation
- Deploying multi-faceted network protection and anomaly detection
- Hardening systems

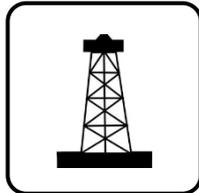
Sector frameworks are customized to the needs of specific industries

Base characteristics

- Designed to address the security concerns of specific business sectors
- Compliance-based frameworks can be customized to provide granular management
 - Specific to meeting operational and regulatory regimens and compliance mandates

Industry Focus

- Initial focus on six sectors, working with government counterparts
 - Financial Services and Banking
 - Energy (Oil & Gas with Energy & Utilities)
 - Transportation
 - Water
 - Healthcare
 - Telecom



Characteristics of organizational frameworks

Base characteristics

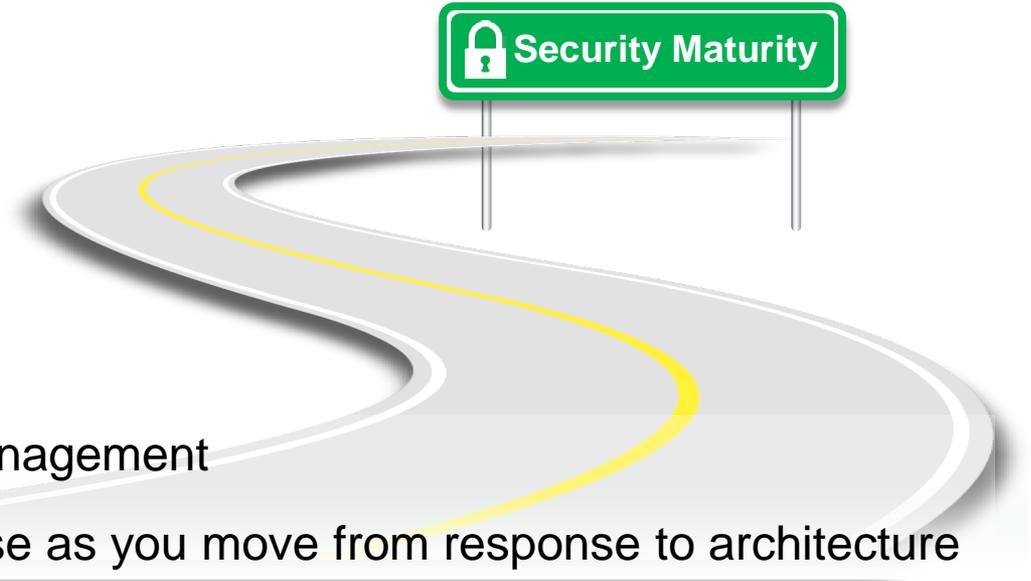
- Generally uses portions of **process**, **domain** and **sector** frameworks
- Based on the organization's business environment and conditions
- Based on evaluations from lines of business / operations, executives, auditors and Board of Directors
- Amends plans based on resources, changing conditions, and new information
- Commonly adopts a customized, organization-based framework based on multiple types

Approach to risk

- Special attention to a limited number of specific approaches for addressing risk and measuring the effectiveness of protection
- Sets the risks, priorities, and risk tolerances for cybersecurity and Information Technology in support of the enterprise
- Examines in even greater detail the overall risk the enterprise faces
 - Determines its unique security requirements
 - Ensures capabilities are in place to provide the necessary security
 - Aligns requirements and technologies with its internal policies and processes

Meets NIST and domain guidelines and Federal, State mandates

Common elements of frameworks



- Each focuses towards risk management
- Technical components increase as you move from response to architecture
- Security frameworks set risk tolerance with stakeholder input and actions
- Security metrics and measurement increase as you move from response to architecture
- Each has a degree of maturity levels / implementation tiers within them
- Each has an assigns a current security profile and should aim for a future security profile

Security frameworks and risk-management strategies address

Evolving threats

Including the growing sophistication of threats, new attack methods, and adaptations to technologies or delivery methods

Changing business needs

Including evolving lines of business, acquisitions, mergers, the integration of operations, and the addition or elimination of business functions

Volatile economics

Including changes in business profitability, the market for the organization's goods or services, national and international economic trends, or wholesale currency changes

Increasing regulation

Including changes and additions to regulation and compliance requirements, locally, nationally or internationally

Technology and process changes

Including adding new or removing existing technologies, or implementing a bring-your-own-device (BYOD) program

Geographic and facilities changes

Including moving to a new location or having data-center or cloud services added from another area

Frameworks lead to a Smart Architecture: Deploying the right technology

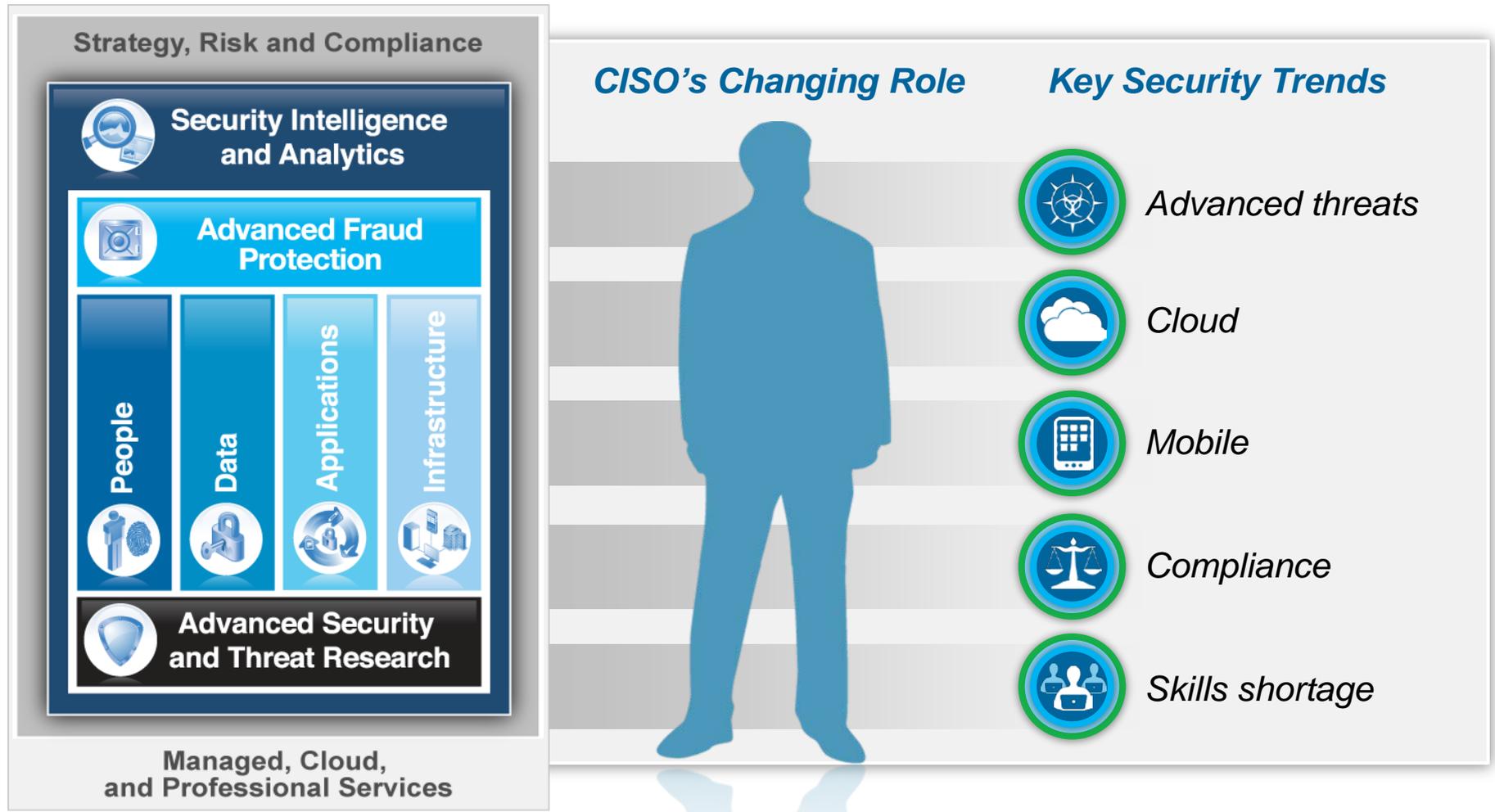
- Uses a risk-based approach accounting for the business operations and conditions of each individual organization and line of business
- Follows the priorities and risk levels set by the organizational risk framework (working group)
- Detailed in scope, policies and active practice
- Tailored by management at all levels
- Includes periodic reviews and reviews on changing conditions

IBM Security Framework



Frameworks flex for Mega Trends

Delivering intelligence, integration and expertise across a comprehensive framework





"The American historian, Barbara Tuchman, in her book *The Guns of August* about the start of the First World War perhaps said it best when she wrote "One constant among the elements of 1914 –as of any era –was the disposition of everyone on all sides not to prepare for the harder alternative, not to act upon what they suspected to be true."

Need some references

- "How mature is your cyber-security risk management?"

http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGW03061USEN&attachment=WGW03061USEN.PDF

- "Applying IBM Security Solutions to the NIST Cybersecurity Framework"

http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGW03064USEN&attachment=WGW03064USEN.PDF

Contact info: Peter Allor pallor@us.ibm.com

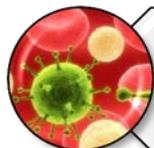
What can you do to mitigate these threats?



Keep up with threat intelligence.



Maintain a current and accurate asset inventory.



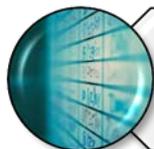
Have a patching solution that covers your entire infrastructure.



Implement mitigating controls.



Instrument your environment with effective detection.



Create and practice a broad incident response plan.

Connect with IBM X-Force Research & Development



Twitter

[@ibmsecurity](https://twitter.com/ibmsecurity) and [@ibmxforce](https://twitter.com/ibmxforce)



IBM X-Force Threat Intelligence
Quarterly and other research reports:

<http://www.ibm.com/security/xforce/>



IBM X-Force Security Insights Blog

www.SecurityIntelligence.com/topics/x-force



Find more on SecurityIntelligence.com

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security



© Copyright IBM Corporation 2014. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.



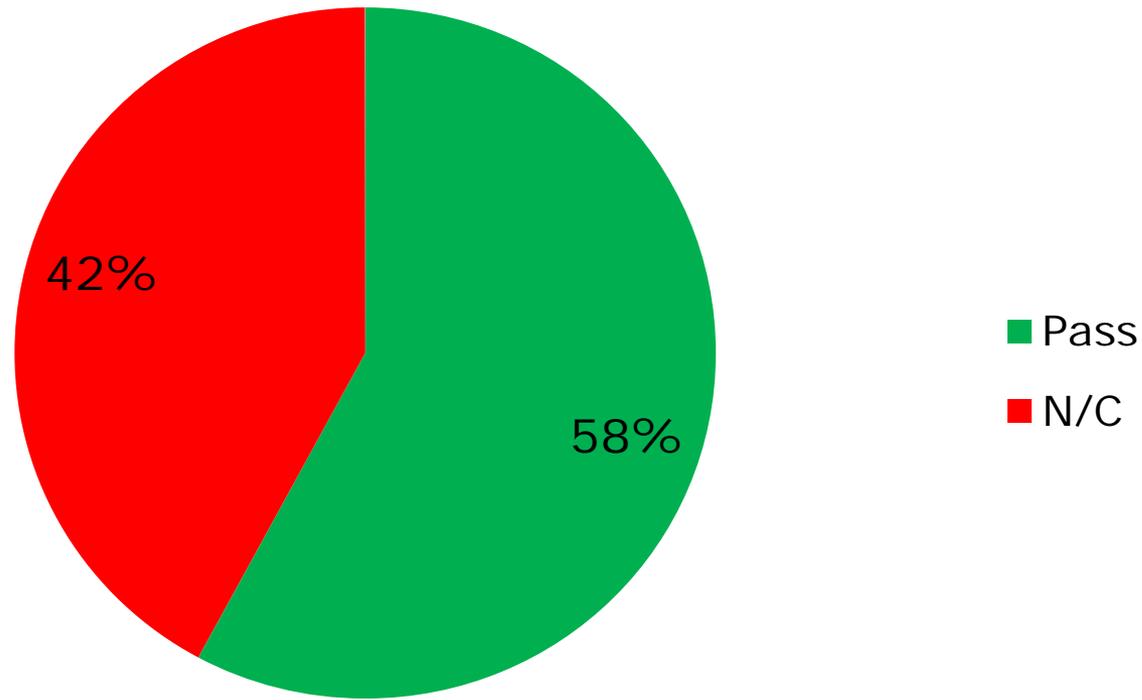
Preview - Draft 2014 Annual Report

Mark Martens
Information Assurance Specialist

ISOAG
April 1st, 2015

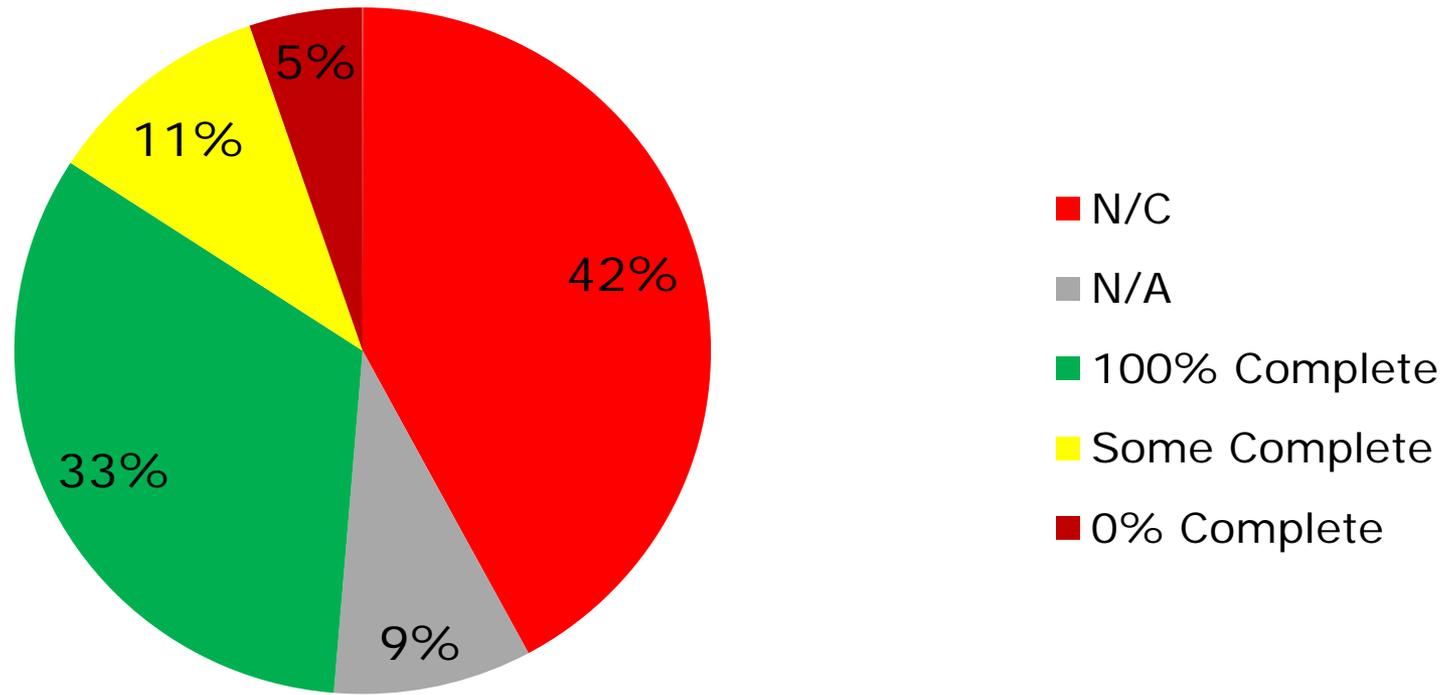
Risk Assessment Plan Status

Risk Assessment Plan Status



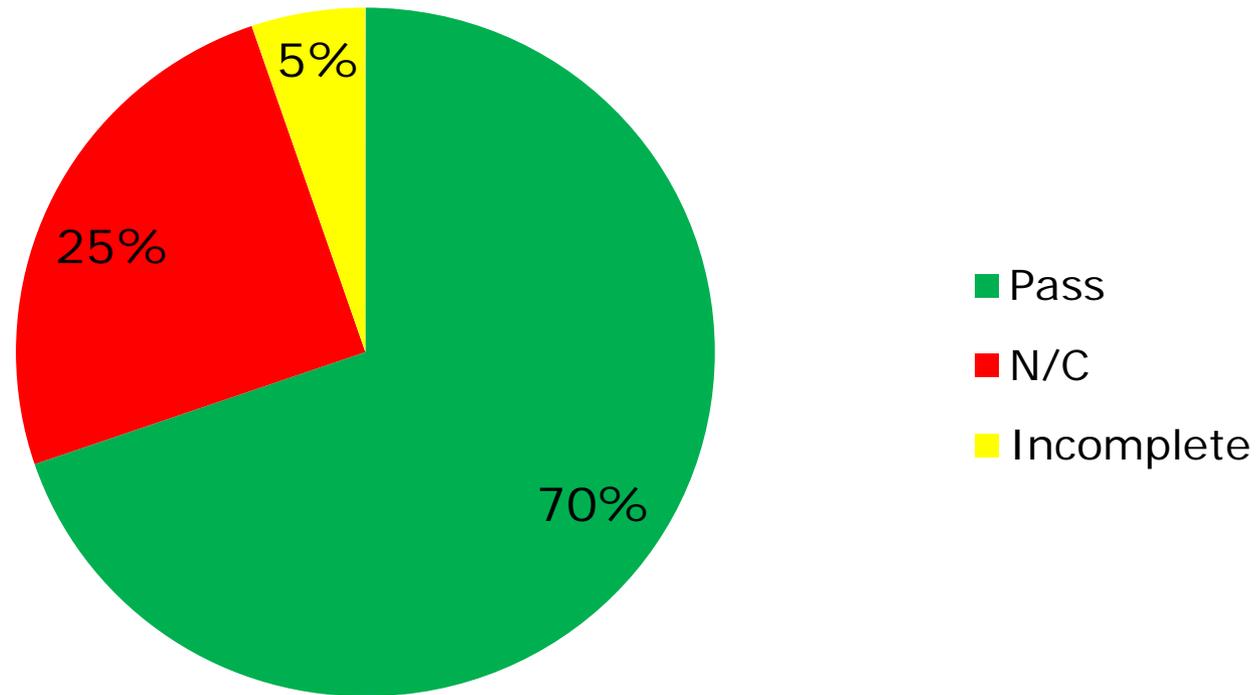
Risk Assessment Obligation

3 Year Risk Assessment Obligation



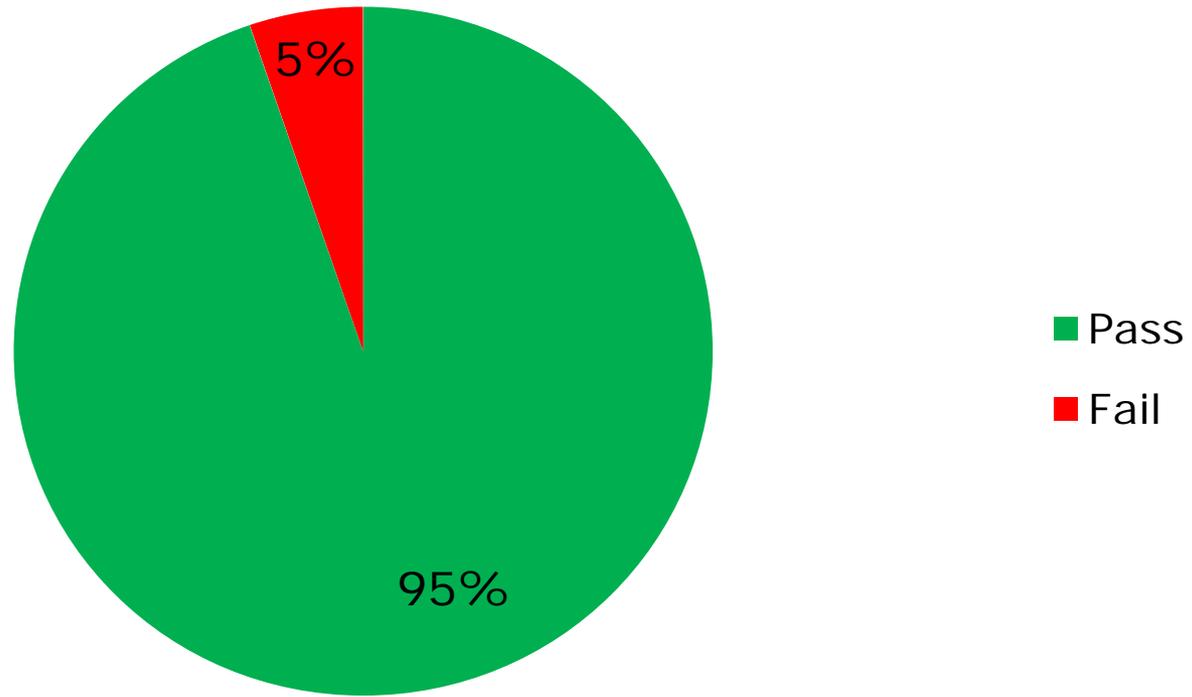
Business Impact Analysis

Business Impact Analysis



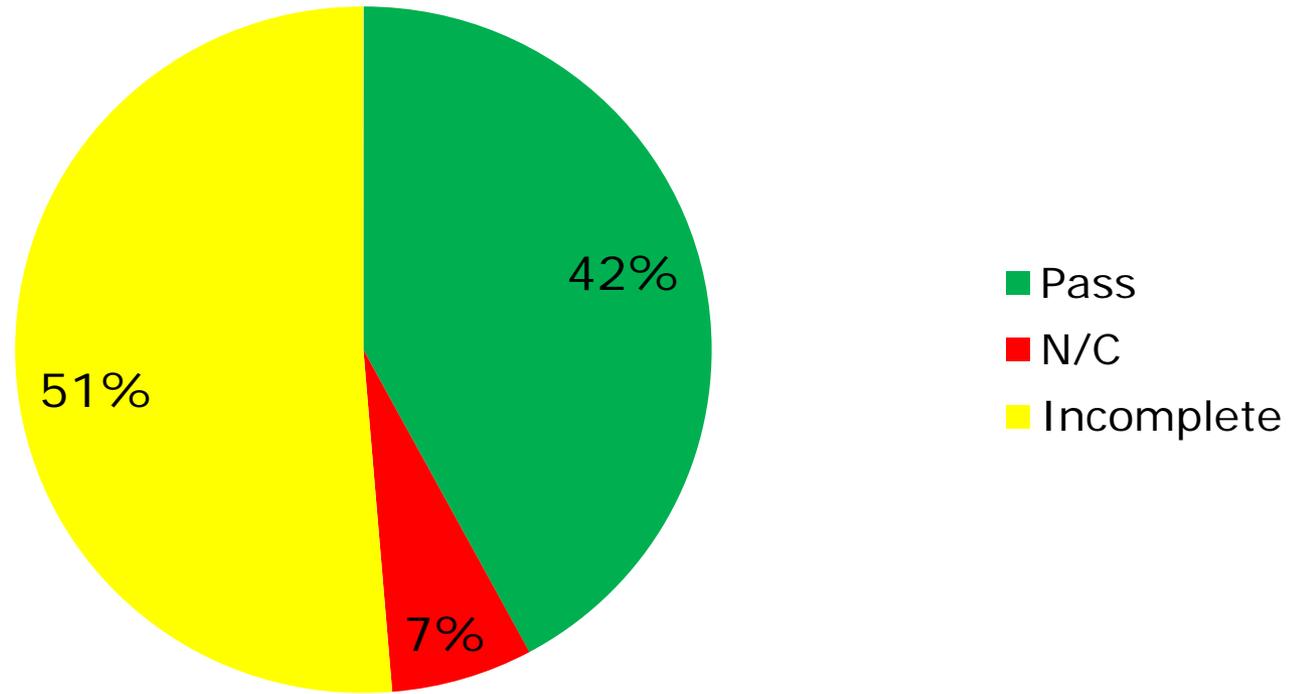
Intrusion Detection Systems

IDS



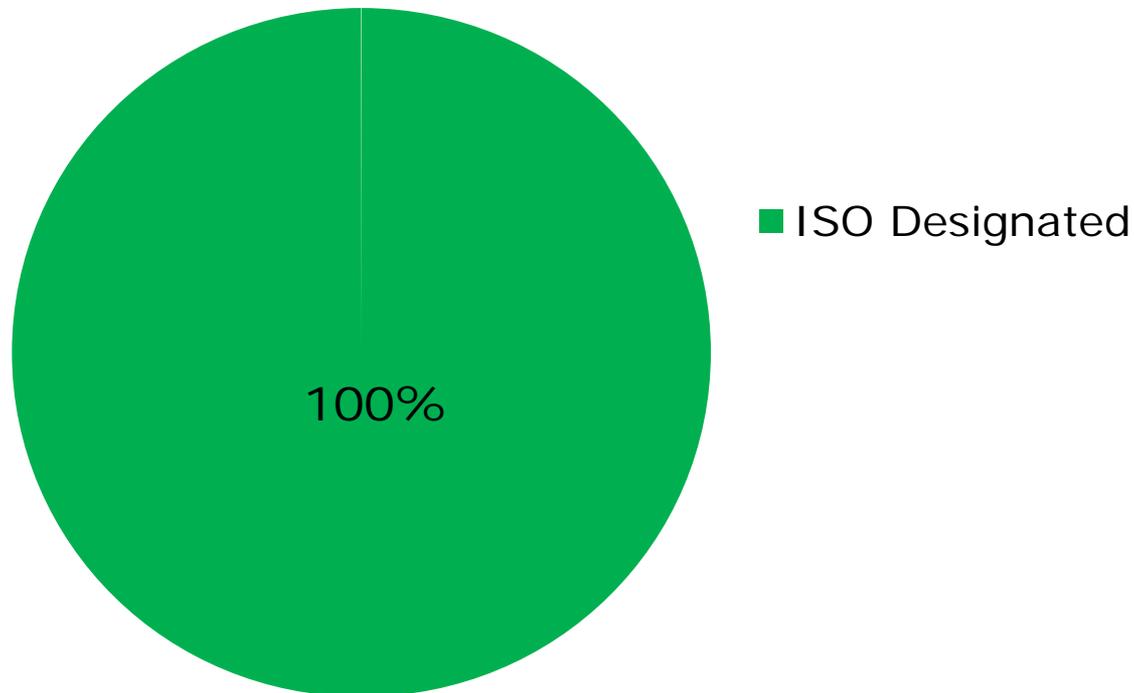
Vulnerability Scanning

Vulnerability Scanning



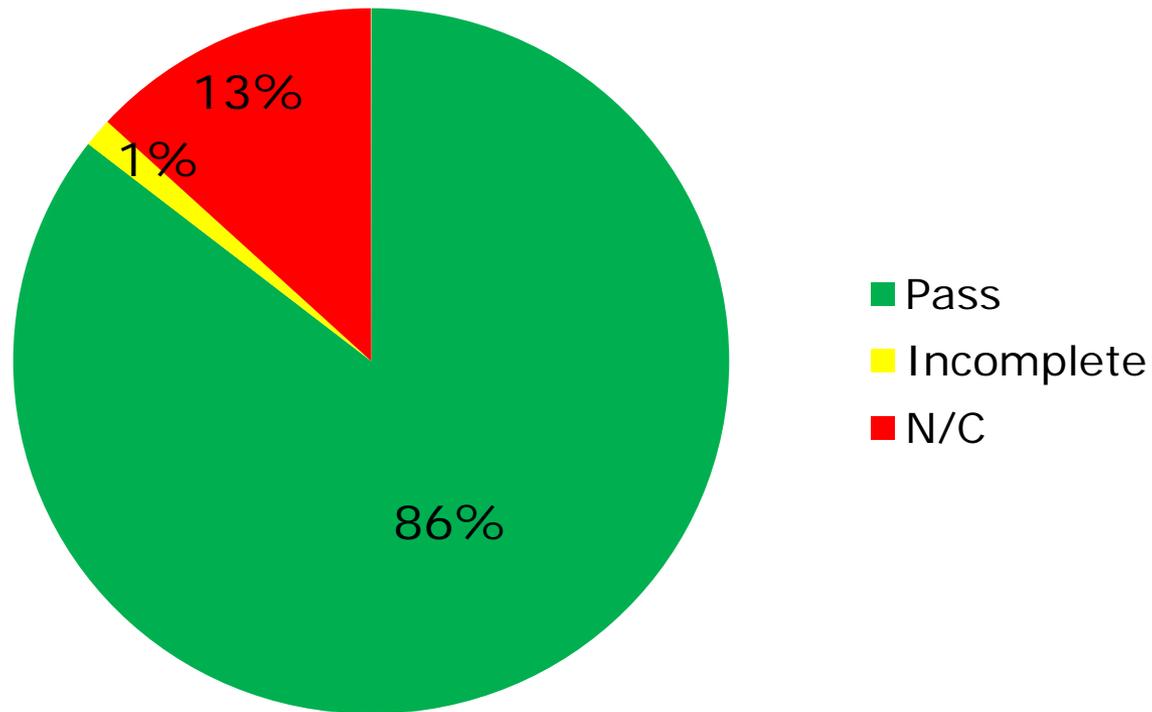
Designation of an ISO

ISO Designation



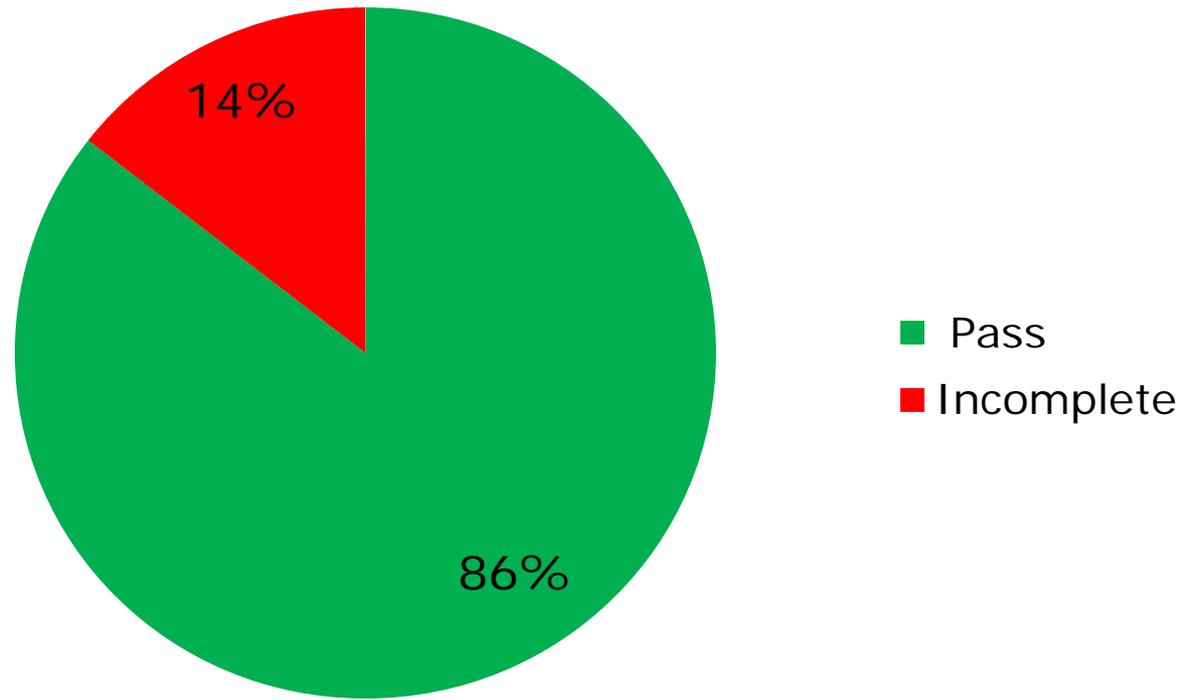
ISO Certification Status

ISO Certification Status



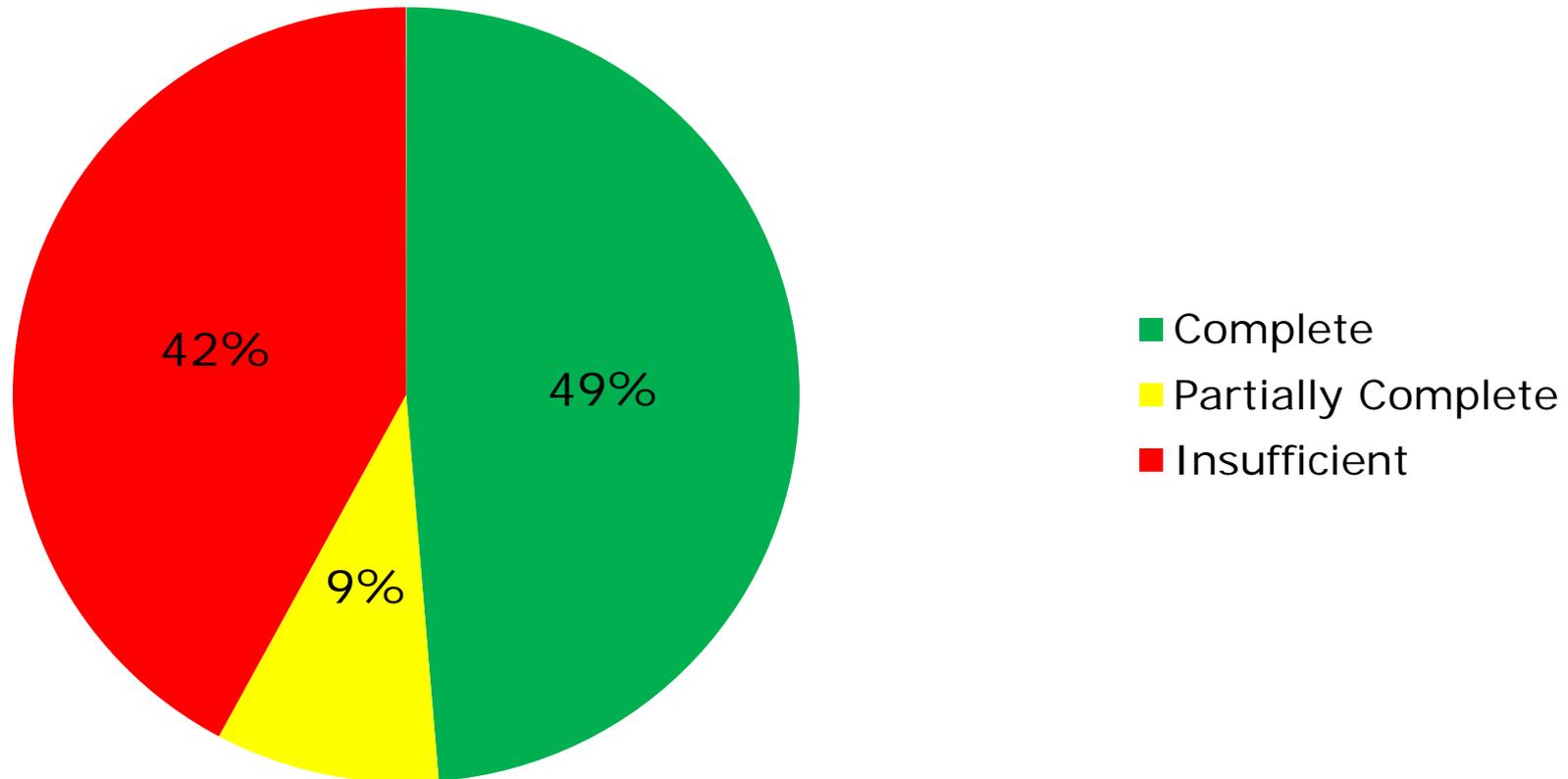
Submission of IT Security Audit Plan

IT Security Audit Plan Status



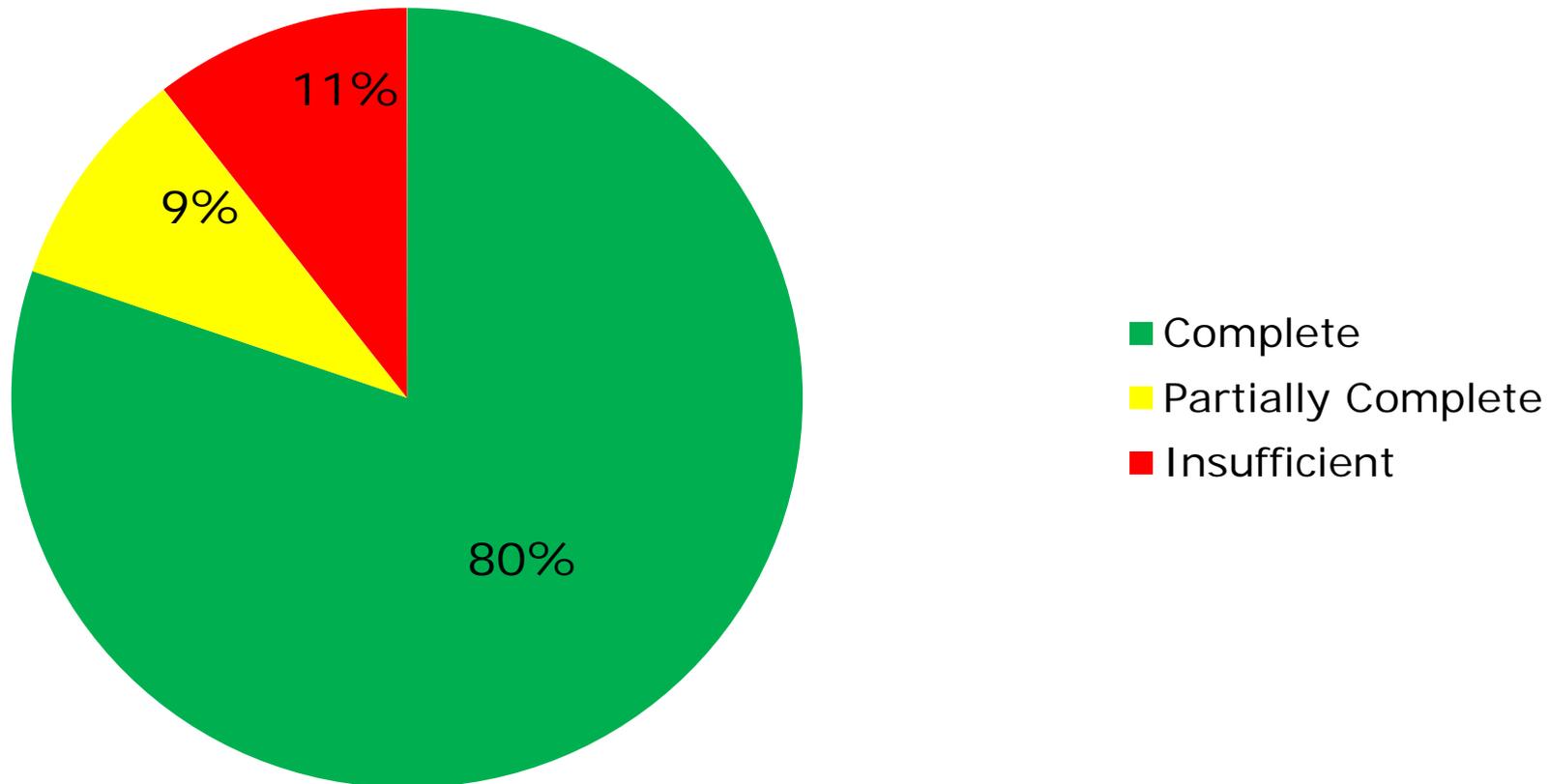
Submission of IT Security Audit Reports

Audits Reports



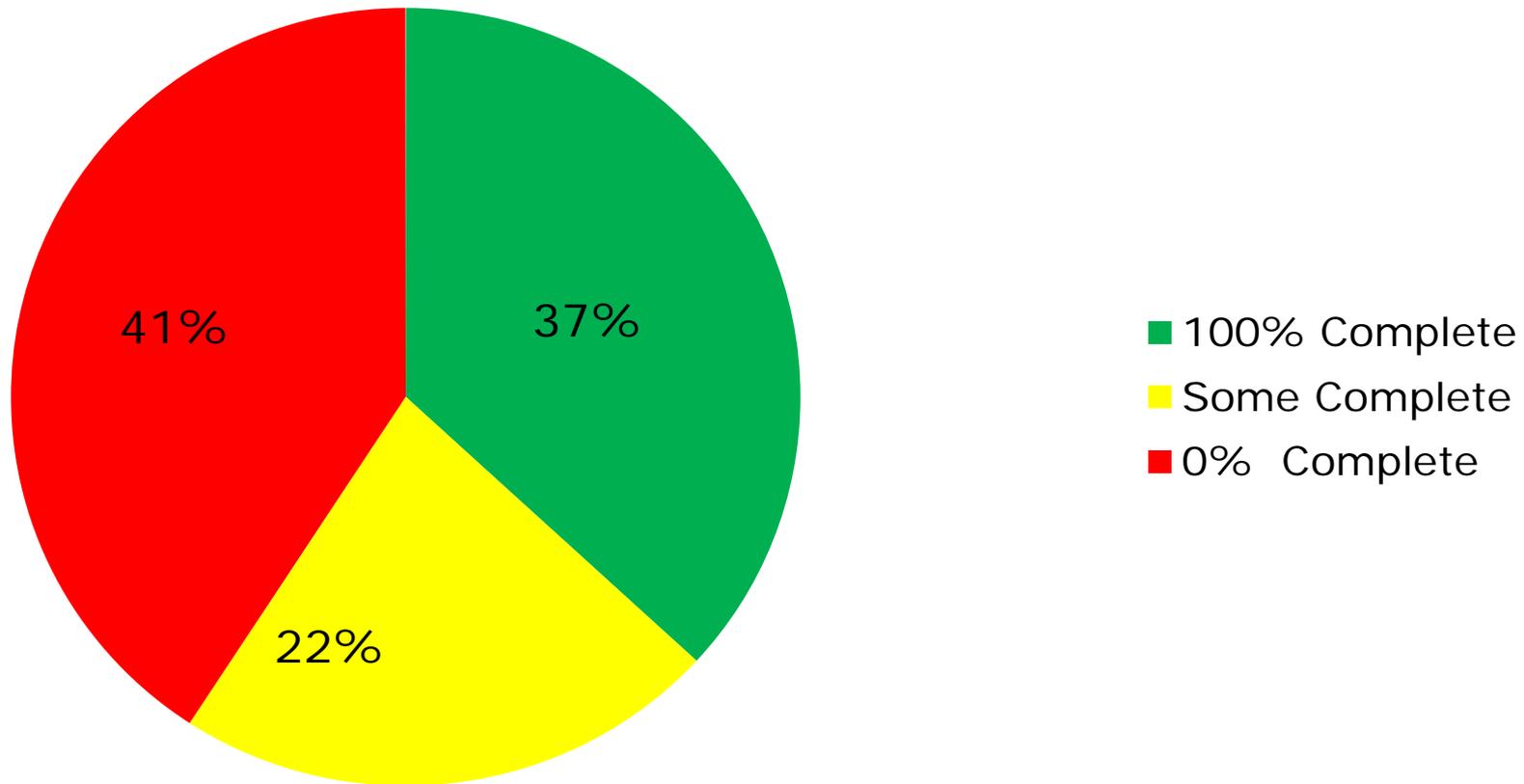
Submission of Quarterly Updates for CAPs

Quarterly Updates



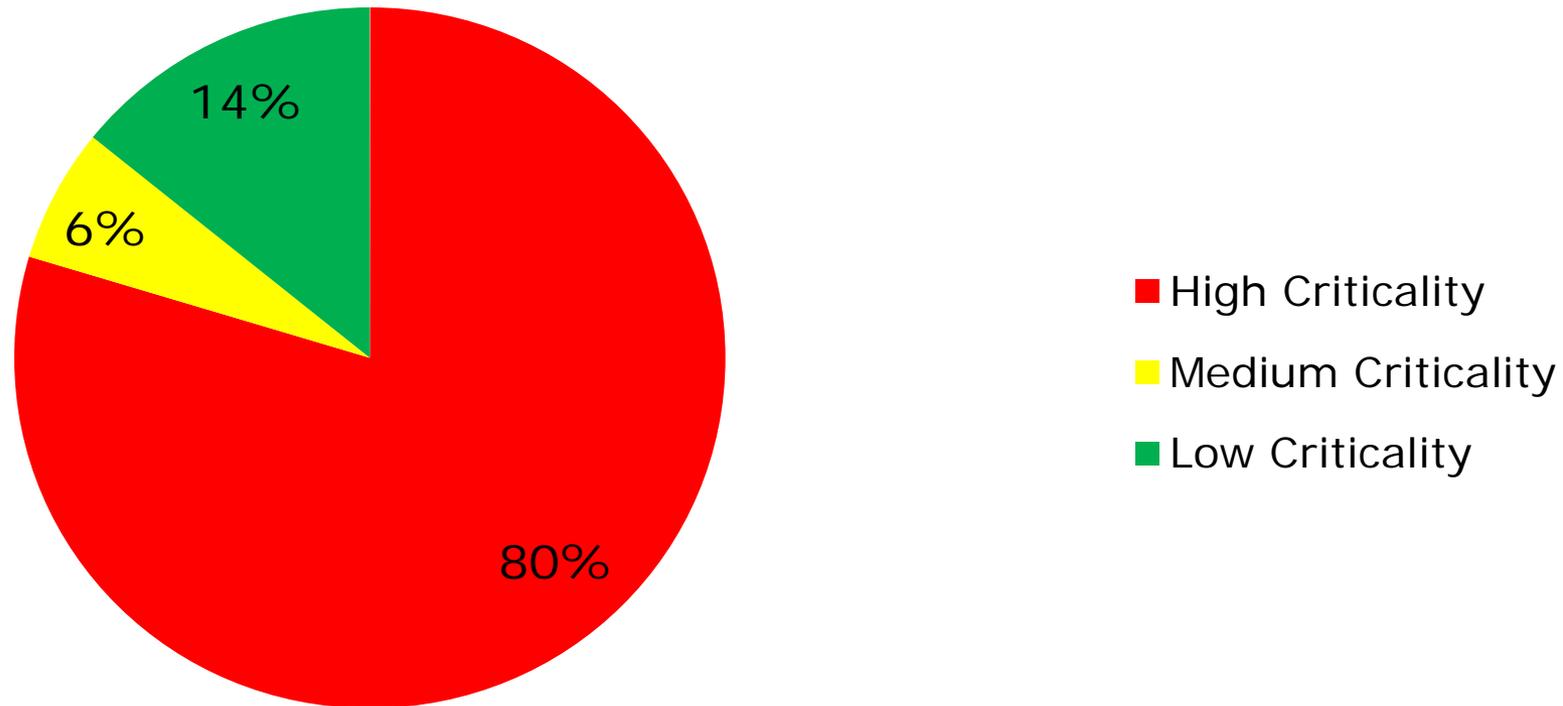
Percentage of Audit Obligation Completed

Audit Obligation



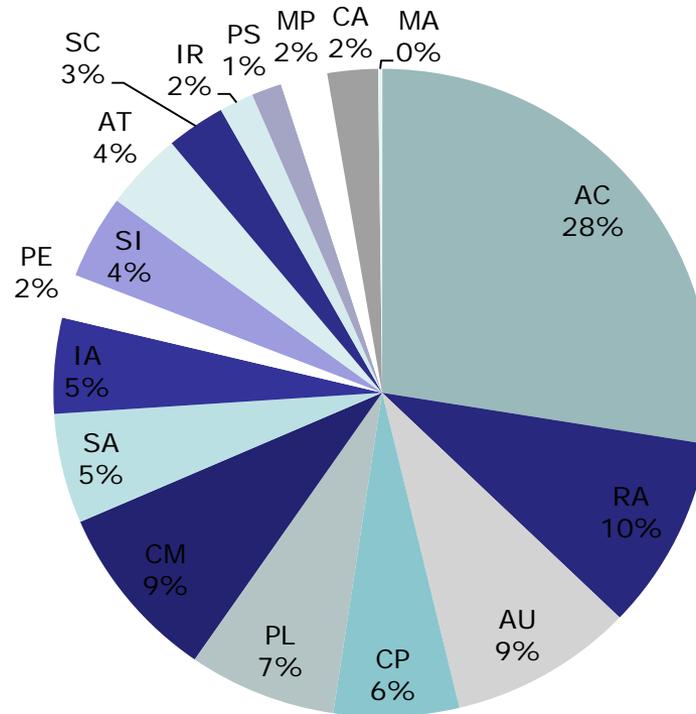
IT Security Audit Findings

IT Security Audit Findings



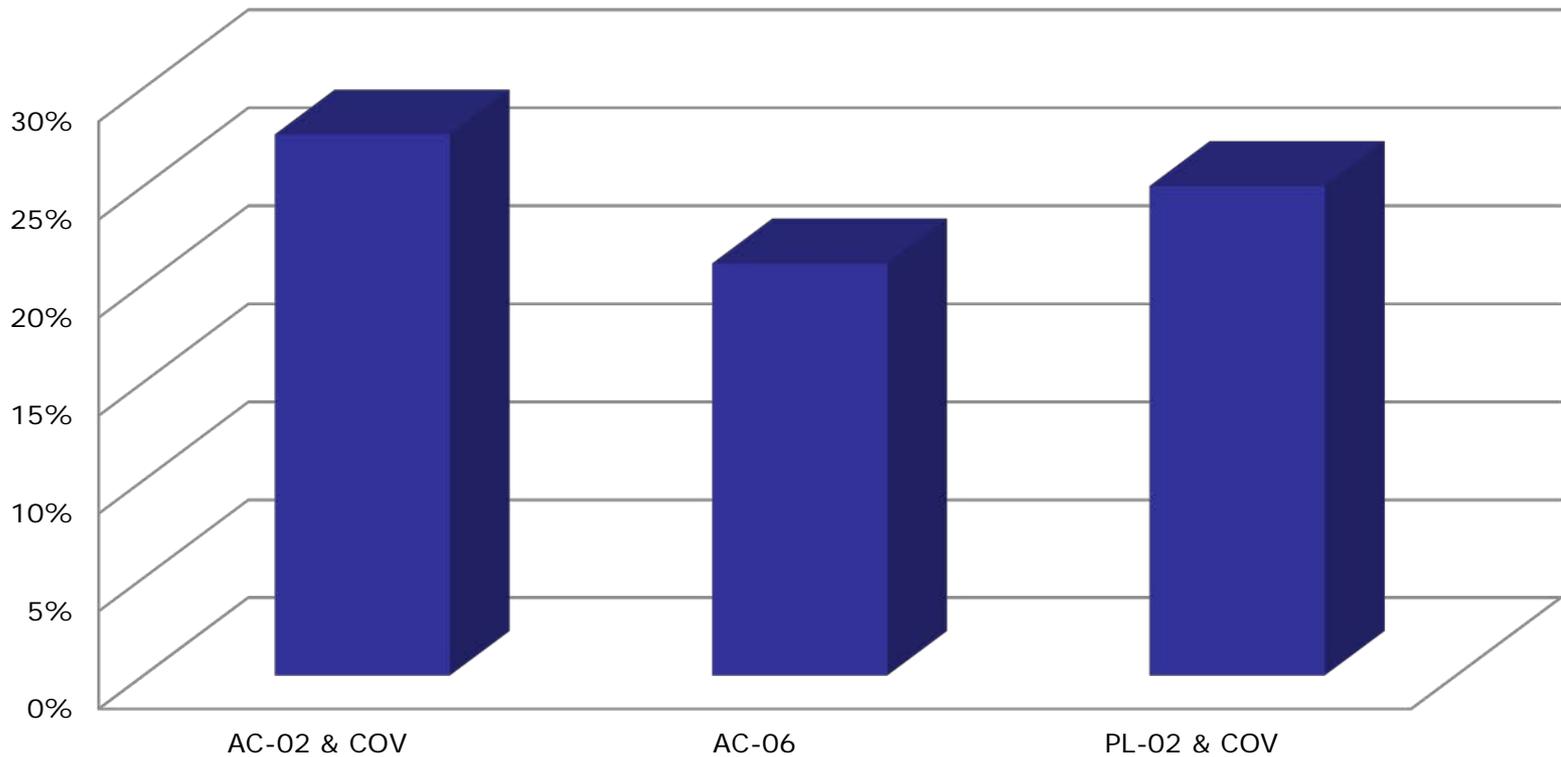
Findings by SEC501 Control

SEC501 Control Findings



Agencies Affected by Top 3 Controls

Top 3 Controls by Agencies Affected

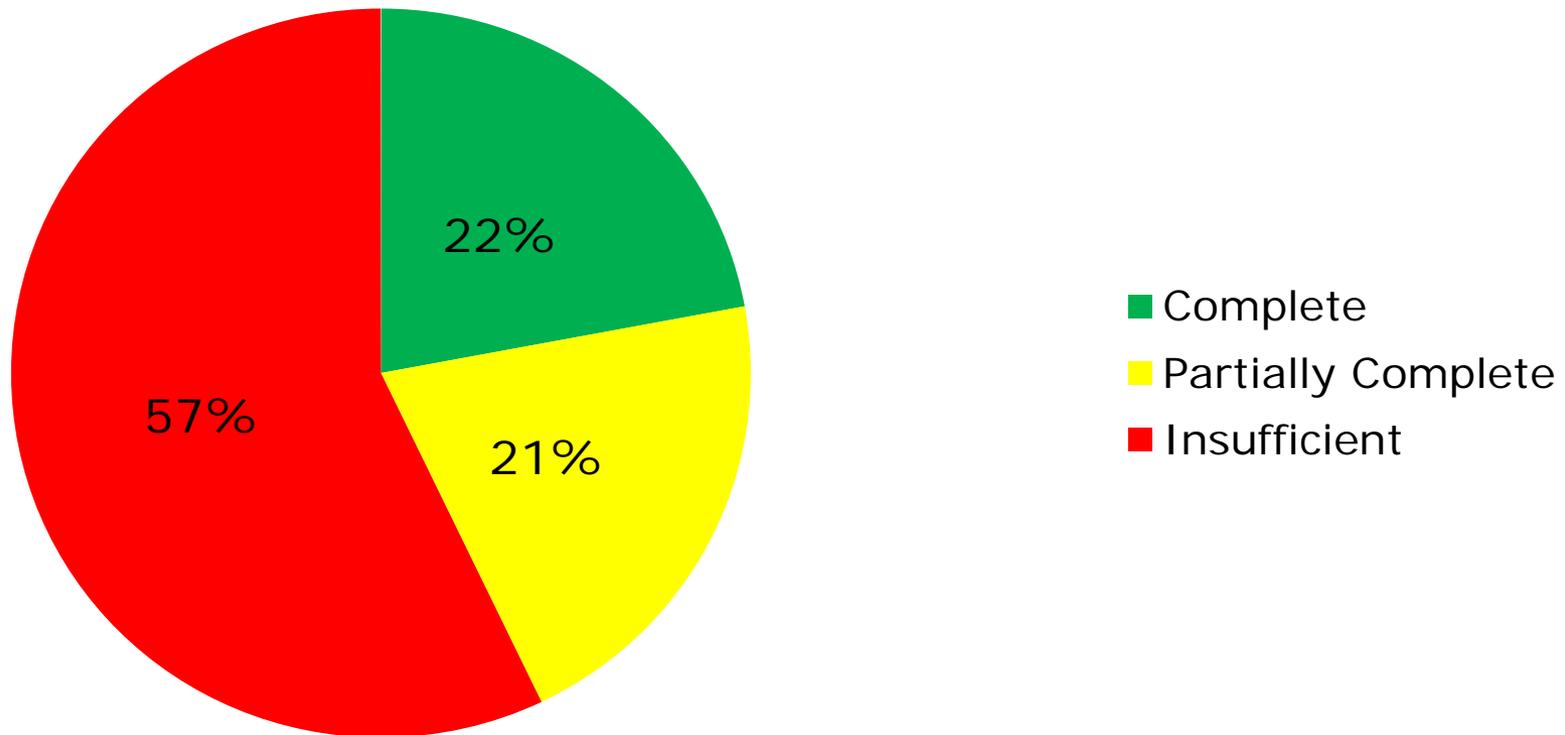


Phishing on the rise

- 2014 – Phishing Incidents made up 31% of all successful attacks. These typically result in unauthorized access of a COV system.
- 2015 1st Quarter – Successful phishing attacks continue to trend up, comprising 35% of all incidents.

Overall Security Audit Program Status

Commonwealth Overall Audit Program Score





Identified Issues

- No noticeable improvement in agency IT security audit programs
 - Agencies are not conducting IT security audits
 - Findings are not addressed in a timely manner
- Agency risk level unknown to executive leadership
 - Lack of IT Security audits and Risk Management practices hinders the ability to determine risk
 - Phishing and Access Control issues are on the rise

Identified Issues (Cont.)

- Software Lifecycle Planning
 - Continued requests for security exceptions for end of life/unsupportable applications
 - About 30 Win2k Servers out there
- Executive Leadership Education
 - Support and resources necessary to implement and maintain an information security program not always available



Questions

????????????????

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



Virginia Information Technologies Agency

Upcoming Events





IS Orientation

When: Thursday, June 16th, 2015

Time: 1:00 pm to 3:00 pm

Where: CESC , Room 1211

Register here:

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>



Future ISOAG

May 6, 1:00 - 4:00 pm @ CESC
Speaker: David Ihrie, CIT

ISOAG meets the 1st Wednesday of each month in 2015



Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to:

CommonwealthSecurity@VITA.Virginia.Gov

ADJOURN

THANK YOU FOR ATTENDING

