Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

September 5, 2012

Virginia Information Technologies Agency

ISOAG September 2012 Agenda

I.	Welcome & Opening Remarks	Michael Watson, VITA
II.	Advanced Persistent Threat	Ben Smith, RSA
III.	EIA COV Data Strategy	Joe Grubbs, VITA
IV.	SEC501.07	Ed Miller, VITA
V.	Cyber Security Month 2012	Ed Miller, VITA
VI.	Upcoming Events & Other Business	Michael Watson, VITA
VII.	Partnership Update	Bob Baskette, VITA Eric Taylor and Michael Clark, NG

Virginia Information Technologies Agency

RSA presentation on Advanced Persistent Threat has been Intentionally Omitted

Virginia Information Technologies Agency

Enterprise Information Architecture (EIA): Commonwealth Data Strategy and the EIA Scorecard

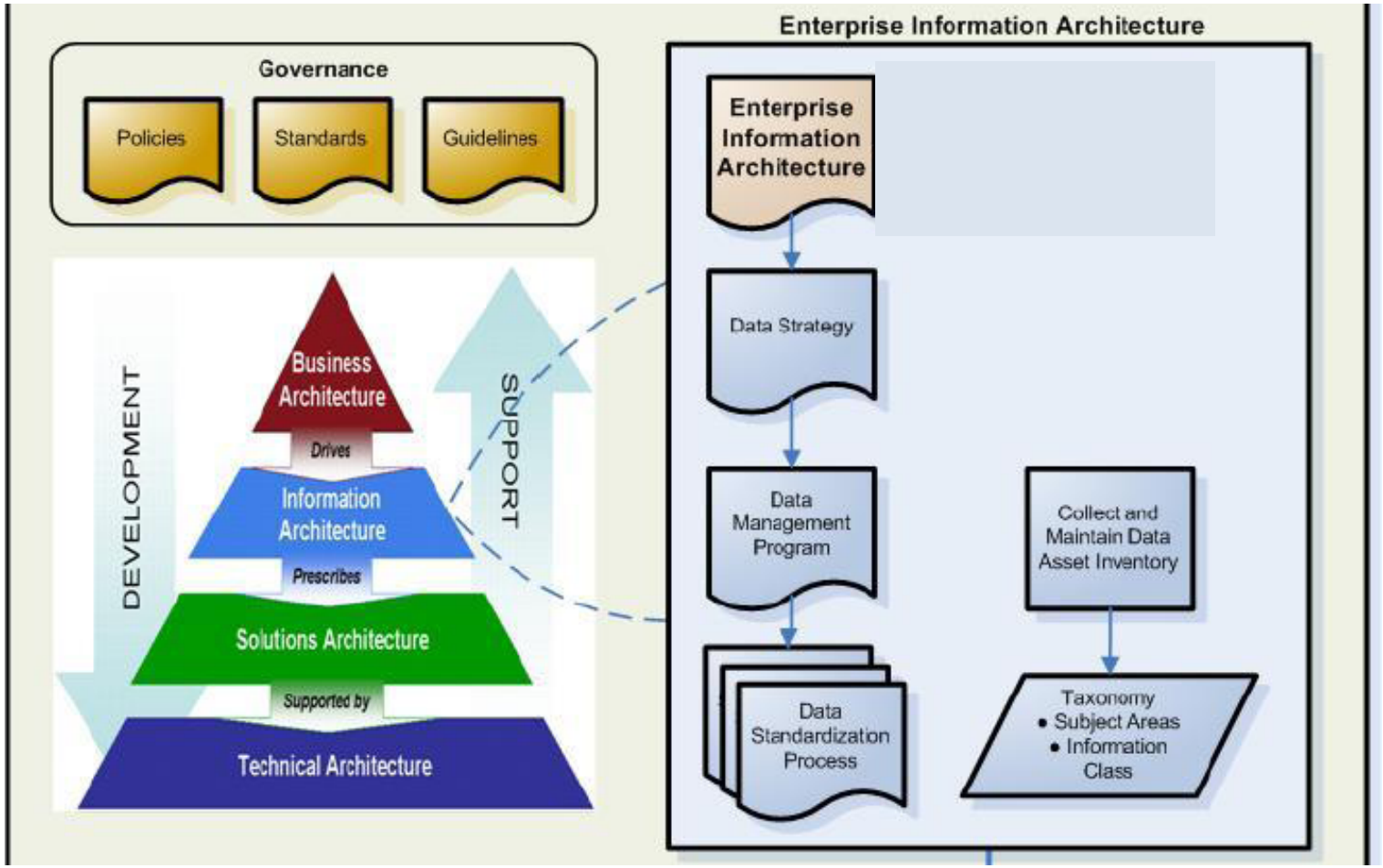
Joseph W. Grubbs, Ph.D.
Commonwealth Data Governance

Presentation Agenda

- Adopted EIA Elements and Maturity Model
- Commonwealth Data Strategy
  - Data Strategy Process
  - EIA Scorecard

EIA Elements & Maturity Model

EA Policy Framework



EIA Elements

- On July 3, 2012, the Secretary of Technology adopted EIA elements to the adopted EA Policy 200-2.
- EIA Elements:
  - More closely align EA Business Architecture with Solutions and Technical Architecture
  - Build upon an EIA Maturity Model to guide the Commonwealth to a desired “future state”
  - Articulate a vision and high-level benchmarks within four EIA program areas

EIA Maturity Model

EIA Program Areas

- *Data Governance*
- *Data Asset Management*
- *Data Standards*
- *Data Sharing*

Informal Level

- Data stored in silos
- Incomplete (if any) metadata or data documentation
- Data non-standardized and built on divergent vocabularies
- Structural barriers to data sharing

Emerging Level

- Coordinating roles starting to emerge for data stewards
- Metadata and documentation for new source systems
- Internal data standards with little interoperability
- Point-to-point data sharing usually within Agency

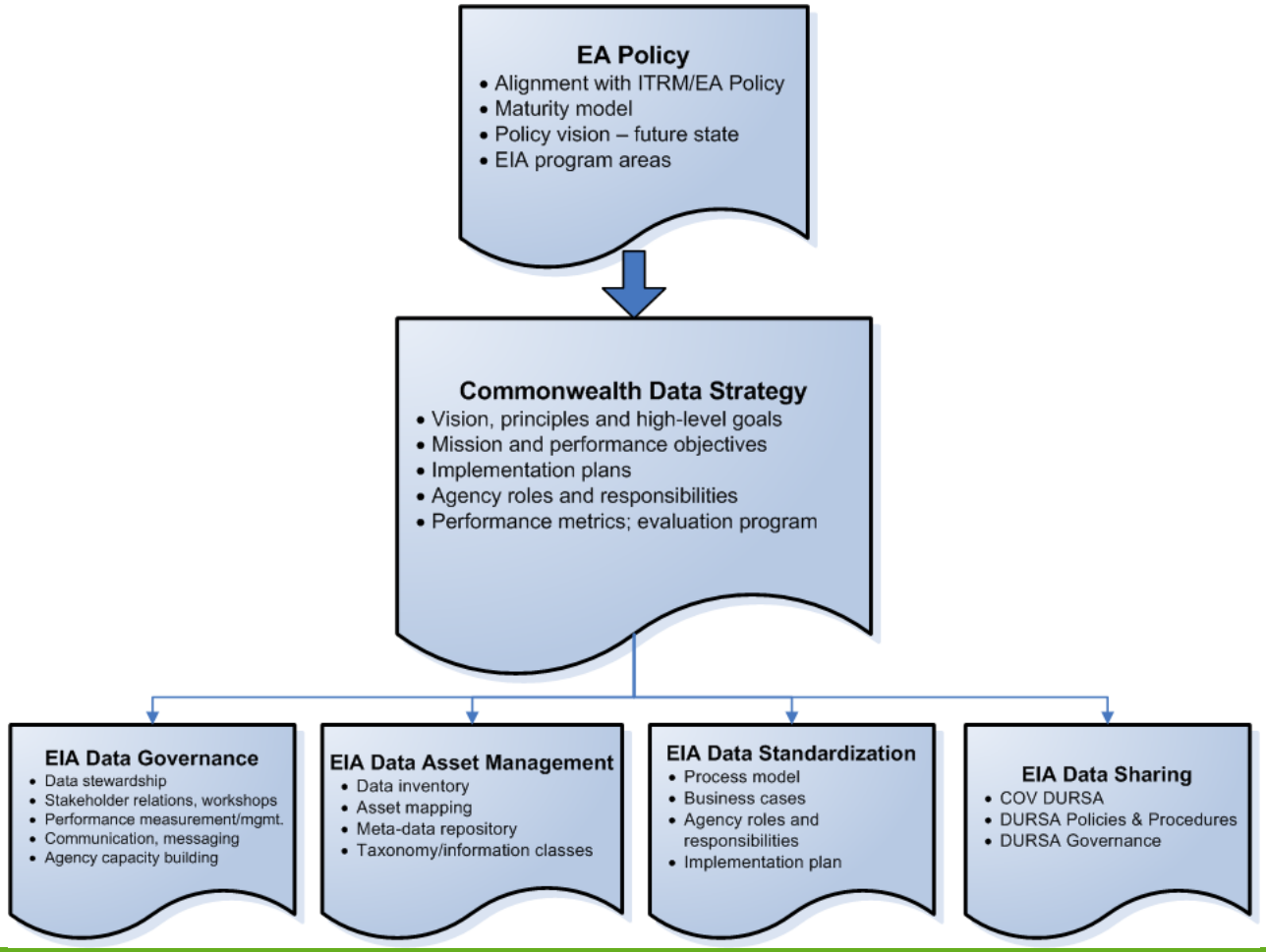
Enterprise Level

- Governance led by enterprise data stewards
- Enterprise-wide metadata repository; taxonomy
- Semantic interoperability supported by external data exchange standards
- Enterprise data-sharing agreement and trust framework

Past State → ***Maturity Curve*** → **Future State**

Graphic Source: AMR Research, 2006

EIA Governance Framework

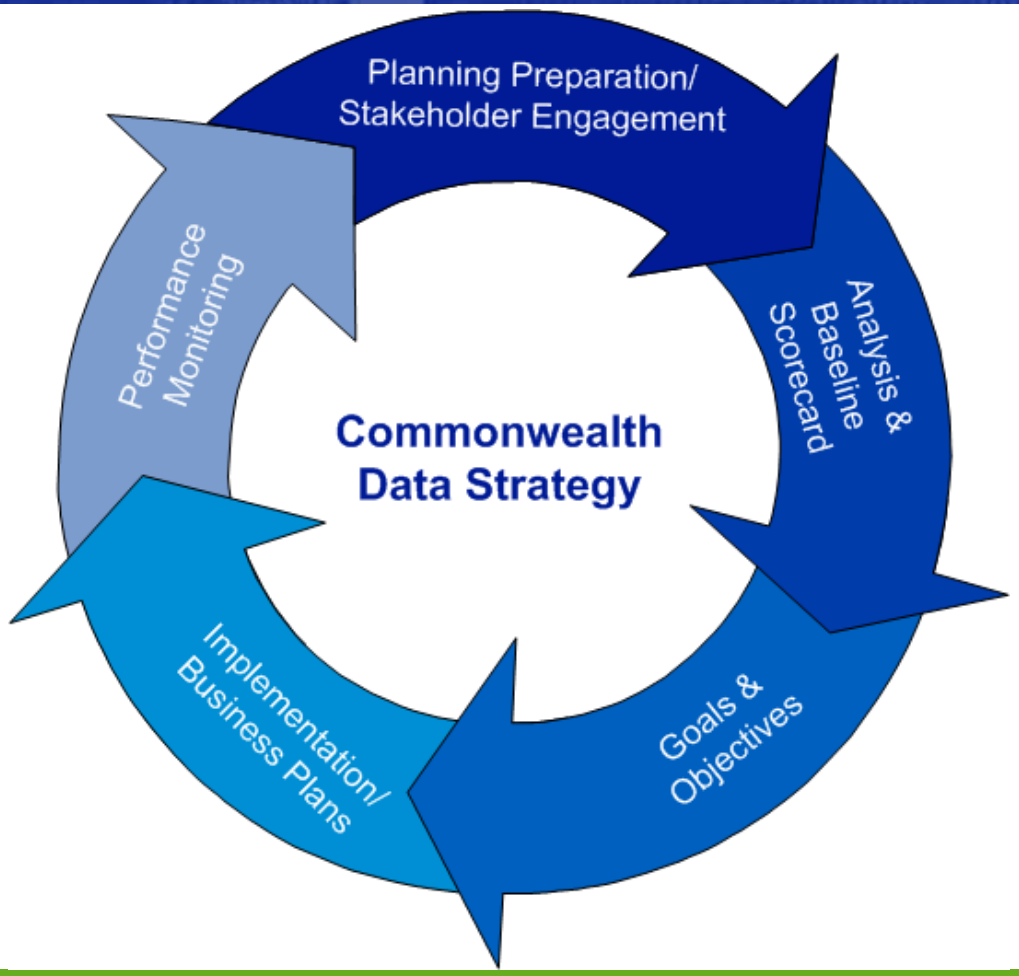


Commonwealth Data Strategy

COV Data Strategy – Purpose

- Develop a COV Data Strategy as the primary driver for implementing the EIA governance framework
- Engage COV data stewards in the Data Strategy process, implementation and performance monitoring
- Use the EIA Scorecard to set measurable goals, objectives and performance targets aligned with the EIA Maturity Model

COV Data Strategy – Process



COV Data Strategy – Process

- Planning Preparation/Stakeholder Engagement
  - Secretariat-level committee/data stewards
- Analysis & Baseline Scorecard
  - Quantitative analysis on EIA Scorecard
  - Identification of performance constraints
- Goals & Objectives
  - High-level EIA goals owned by data stewards
  - Performance targets in primary EIA programs

COV Data Strategy – Process

- Implementation/Business Plans
  - Implementation strategies at the Agency, program and data system level
  - Performance metrics tied to strategies and aligned with EIA program areas
- Performance Monitoring
  - Ongoing application of EIA Scorecard
  - Evaluation of progress along EIA Maturity Curve based on performance metrics

Questions?

Joseph W. Grubbs, Ph.D.
Enterprise Information Architect
Commonwealth Data Governance
Virginia Information Technologies Agency
Phone: (804) 416-6171
Email: *Joseph.Grubbs@vita.virginia.gov*

Virginia Information Technologies Agency

Welcome
To
The Families!

An Introduction to SEC501-07

Ed Miller
Security Analyst

Agenda

- **WHAT** is NIST?
- **WHY** do we want to use NIST?
- **HOW** do we use NIST?
- **WHEN** will this happen?
- **QUESTIONS?**

New SEC501-07

- CSRM has been involved in a substantial rewrite of the Commonwealth's Information Security Standard (SEC501).

- The new version of the Standard has been broadened to include security best practices in line with the **National Institute of Standards and Technology (NIST)** specifically **NIST 800-53**.

First of all, what is NIST?

- The **National Institute of Standards and Technology** (**NIST**), is a measurement standards laboratory, which is a non-regulatory agency of the United States Department of Commerce.

- The institute's official mission is to:

- *"Promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life."*

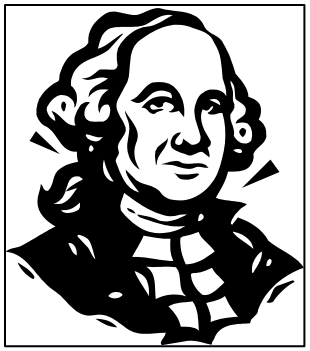
History of NIST

- 1789: Article 1, section 8, of the **Constitution** of the US:

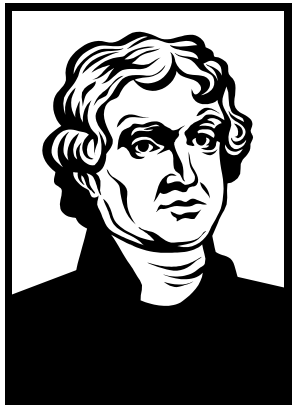
  "The Congress shall have power ... to coin money, regulate the value thereof, and of foreign coin, and fix the standard of weights and measures”.

History of NIST

- 1790: President **George Washington**, in his first annual message to Congress stated that, "Uniformity in the currency, weights, and measures of the United States is an object of great importance, and will, I am persuaded, be duly attended to".



- Washington then ordered Secretary of State **Thomas Jefferson** to prepare a plan for "Establishing Uniformity in the Coinage, Weights, and Measures of the United States".



History of NIST

- 1830: The federal **Office of Weights and Measures** was formed & given the role of overseeing weights and measures.

- 1901: The "Office of Weights and Measures“ was renamed to the "**National Bureau of Standards**”.

- 1988: National Bureau of Standards was reorganized to become the “**National Institute of Standards and Technology” or NIST** (part of Dept of Commerce).

NIST Organization

NIST's activities have broadened over the years to include standardization of measurements & research in many areas.

- Time standards
- Drugs/pharmaceuticals
- Food labeling
- Clothes sizes
- Radiation dosages
- DNA/genetics
- Fire safety/building code
- GPS
- Weather forecasting
- Laser lights
- Energy/fuel
- AC/Refrig Thermo Stds
- Electronic Voltage Stds
- Aviation
- Chemical
- Atoms/Molecular/Nanotech
- Material composition stds
- Military standards for bullet proofing, ballistic calibration
- Data encryption
- Optics
- And many others

NIST Organization

NIST manages these various areas of standards and research by organizing itself into departments that it calls **"laboratory programs".** NIST Laboratories include:

- Engineering Laboratory (EL)
- **Information Technology Laboratory (ITL)**
- Material Measurement Laboratory (MML)
- Physical Measurement Laboratory (PML)
- Center for Nanoscale Science and Technology (CNST)
- NIST Center for Neutron Research (NCNR)

Information Technology Laboratory (ITL)

- The **Information Technology Laboratory (ITL)** consists of several divisions:
  - Applied and Computational Mathematics
  - Advanced Network Technologies
  - **Computer Security**
  - Information Access
  - Software and Systems
  - Statistical Engineering

What is the NIST 800 Series?

- NIST ITL Computer Security Division has published a series of information security "Special Publications", i.e. guidelines and documents:
  - Collectively known as "NIST 800 Series"
  - http://csrc.nist.gov/publications/PubsSPs.html/
- The 800 Series covers a wide spectrum of topics:
  - risk assessments, wireless security, encryption, telecommuting, password management, etc.
- The documents are free of charge & have become increasingly utilized by state & local government agencies as well as businesses & educational institutions.

NIST SP 800-53

- One of the most important guidelines in the 800 series is **NIST SP 800-53 "Recommended Security Controls for Federal Information Systems and Organizations"**.

- 800-53 provides guidance on how to identify the security controls (baseline) needed for information systems. It includes a **master catalog of security requirements** that are non operating system specific and suitable for both legacy and newer systems.

- 800-53 is the framework used for the new SEC501-07.

Why should we adopt NIST 800-53?

Adoption of a well-known and internationally recognized framework of information security controls for the Commonwealth offers several advantages.

Why adopt NIST 800-53?

- Having all agencies use a nationally standardized IT security framework will provide greater insight into the overall security posture of the Commonwealth and will tell us how we compare to the federal government, other states and also private industry.

Why adopt NIST 800-53?

- Using NIST 800-53 as our security requirements framework allows the Commonwealth to leverage research already performed & implementation guidance already produced by the federal government.

- It also provides the opportunity for better alignment between state and federal security requirements.

Why adopt NIST 800-53?

- Many federal agencies are now requiring "**NIST compliant**" documentation of IT security for federally funded projects or for collaborations.

- The Department of Homeland Security strongly encourages any state or local government agency or private organization that comprises part of the **critical infrastructure of the nation** to use the guidelines of NIST 800-53.

Why adopt NIST 800-53?

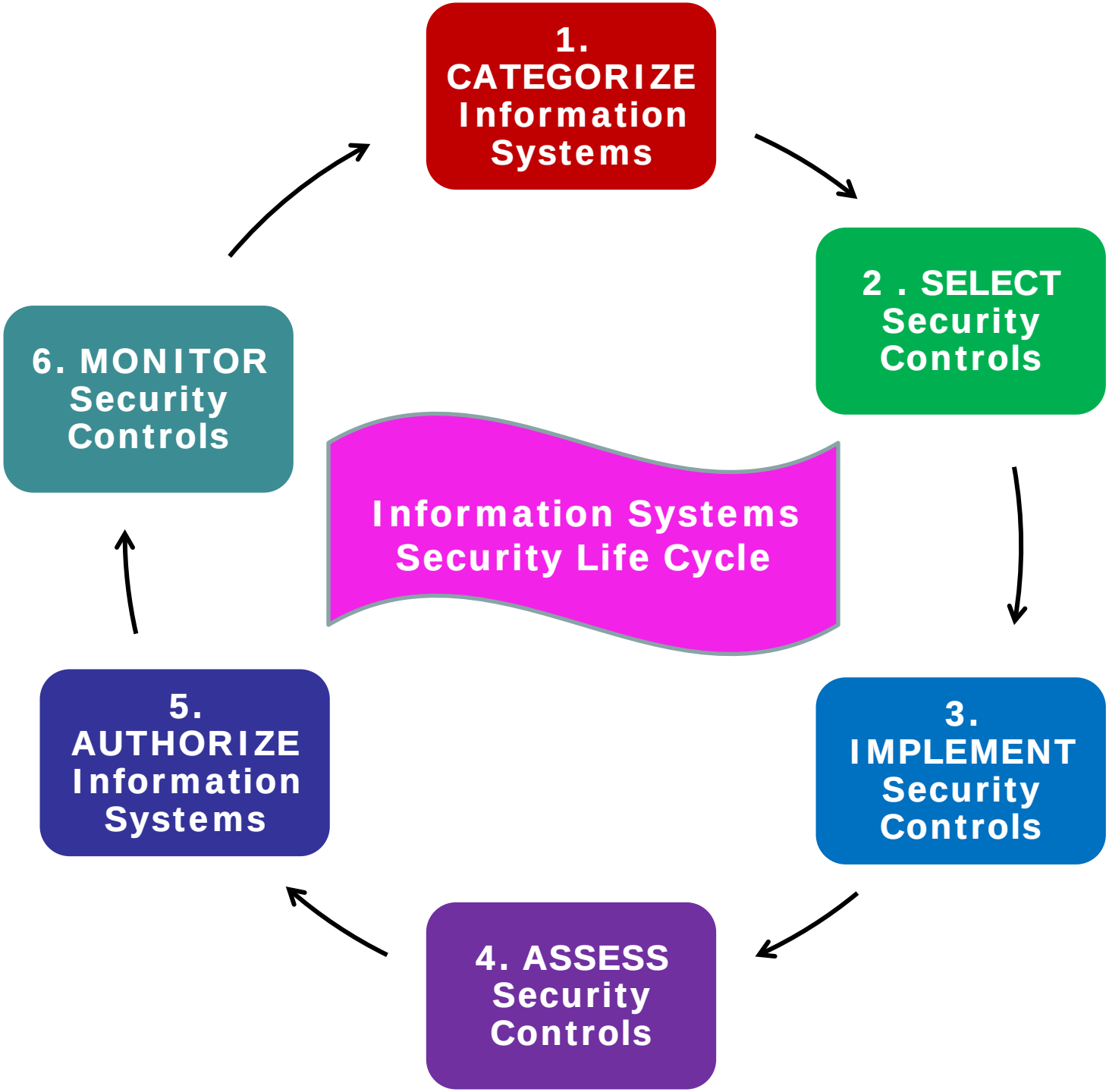
- Many of the NIST SP 800-53 Security Controls align closely with the requirements, controls & guidance of:
  - ISO 27002
  - HIPAA
  - COBIT
  - Sarbanes-Oxley
  - Gramm-Leach-Bliley

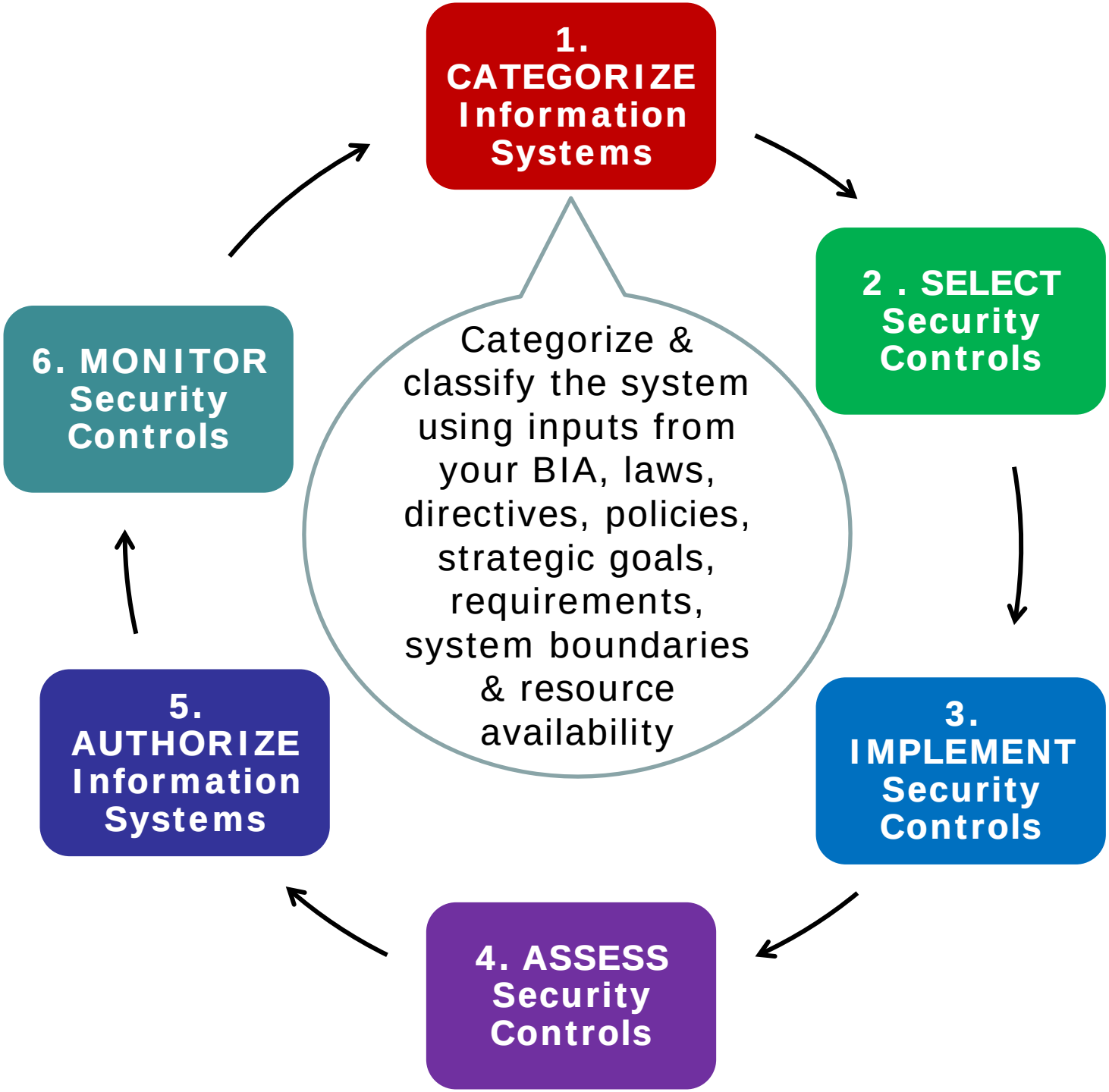
Why adopt NIST 800-53?

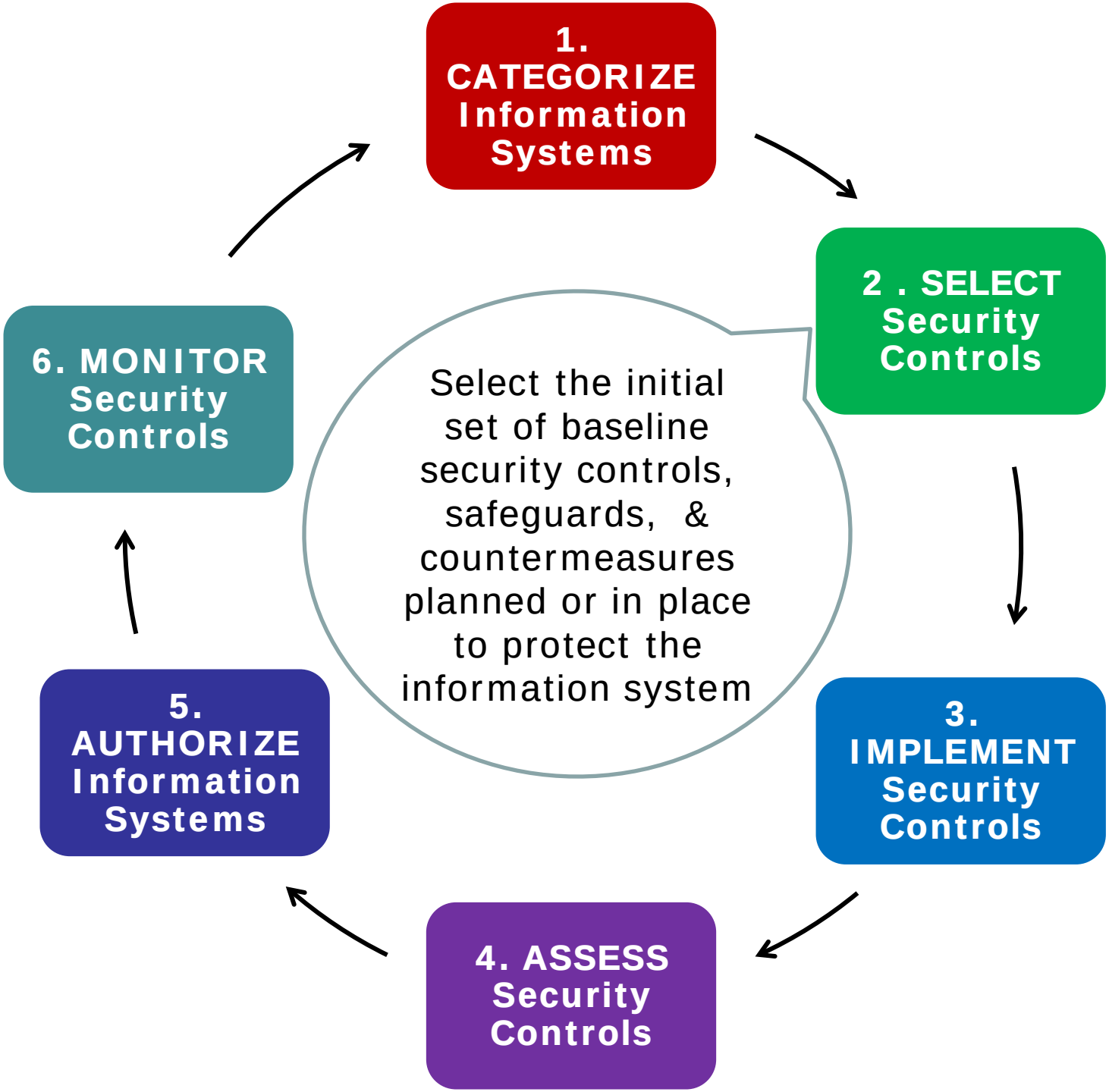
- The flexibility & security requirement crossover of NIST 800-53 with other frameworks will allow agencies that may be subject to many different requirements to address them all within a single methodology.

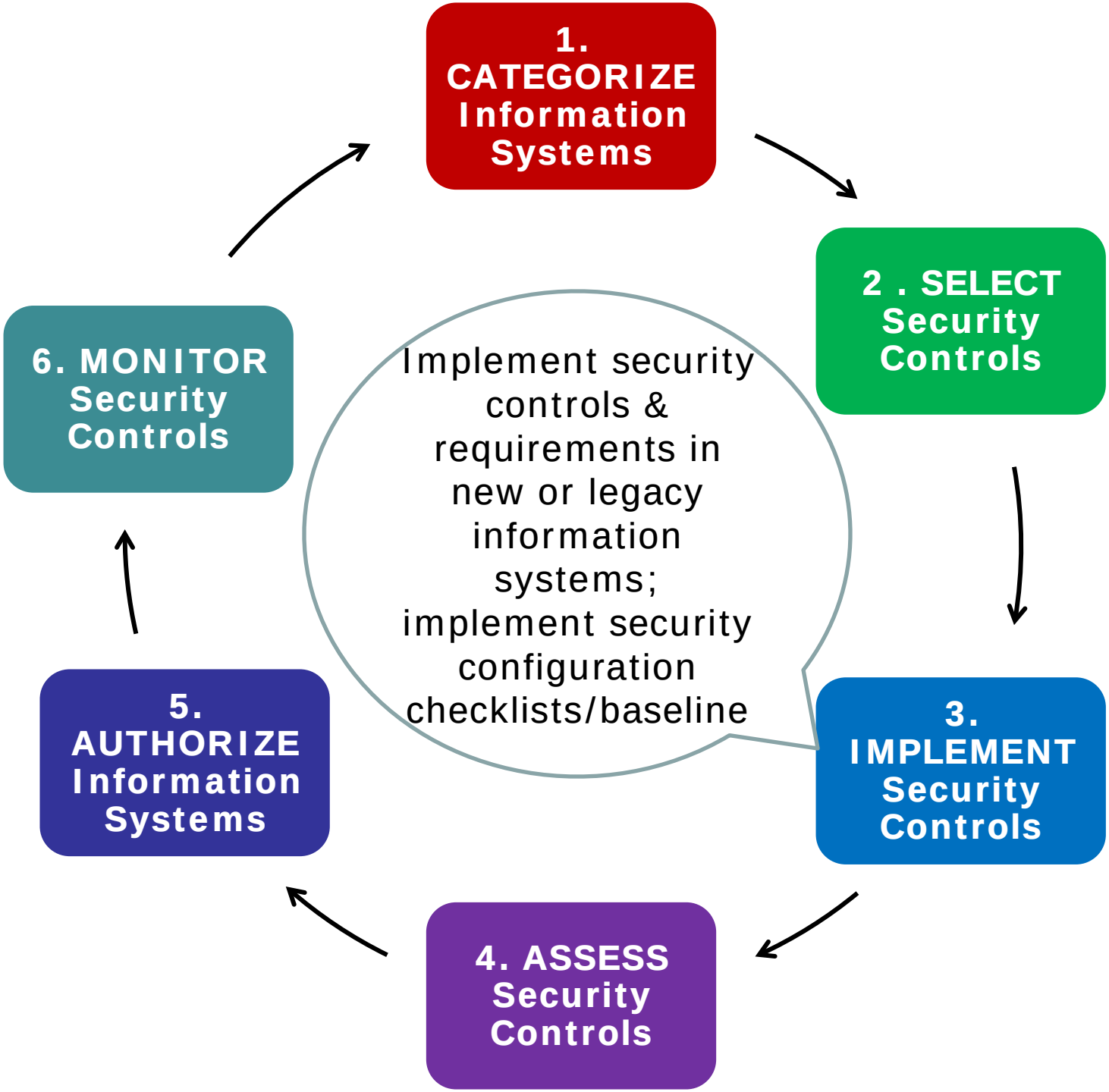
Information System Security Life Cycle

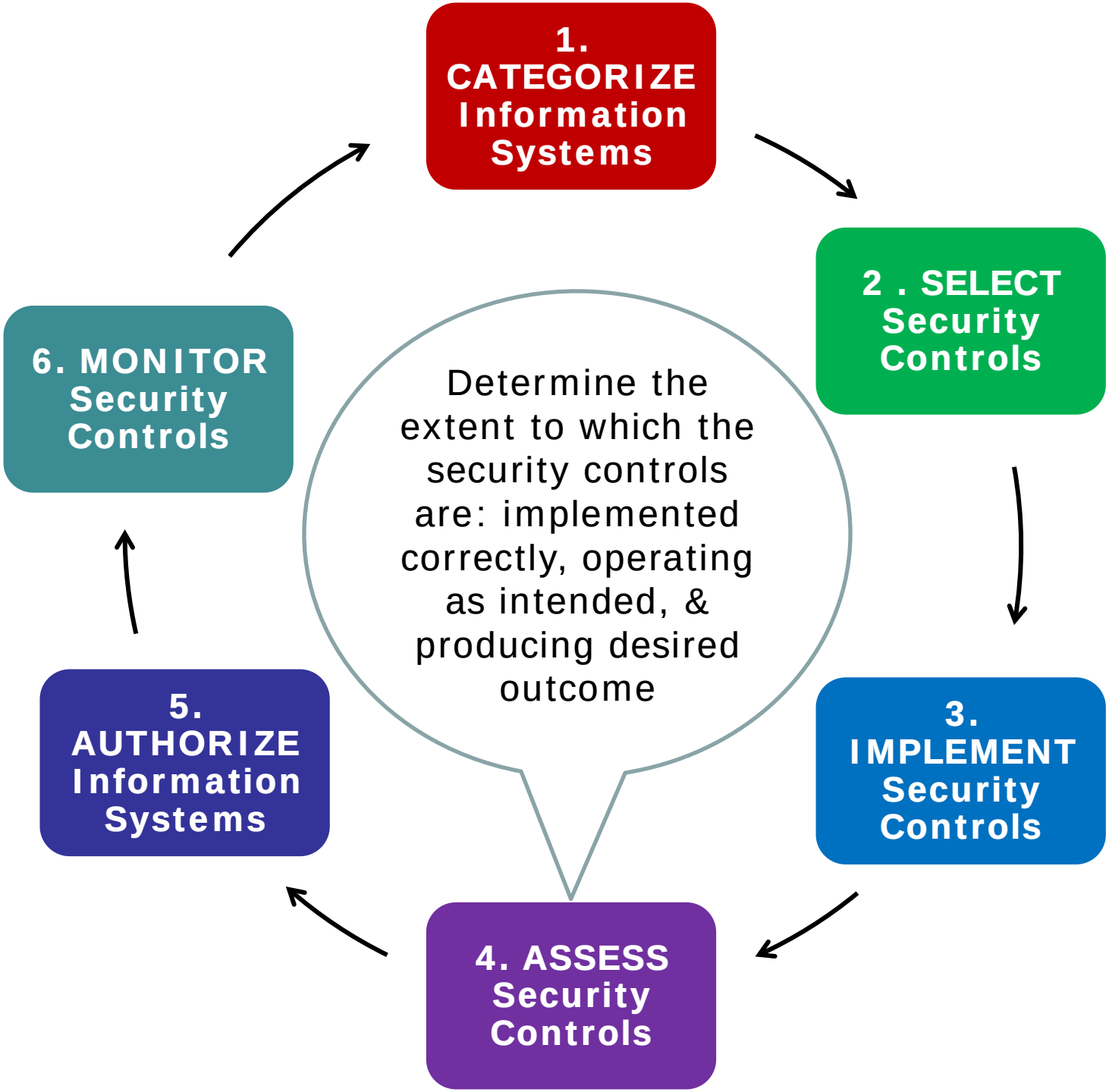
- Properly utilizing NIST 800-53 requires that agencies adhere to a continuous **life cycle** for managing the security of information systems:
  - **Categorize** the system
  - **Select** security controls
  - **Implement** security controls
  - **Assess** the effectiveness of security controls
  - **Authorize** the use of the system
  - **Monitor** the system continuously

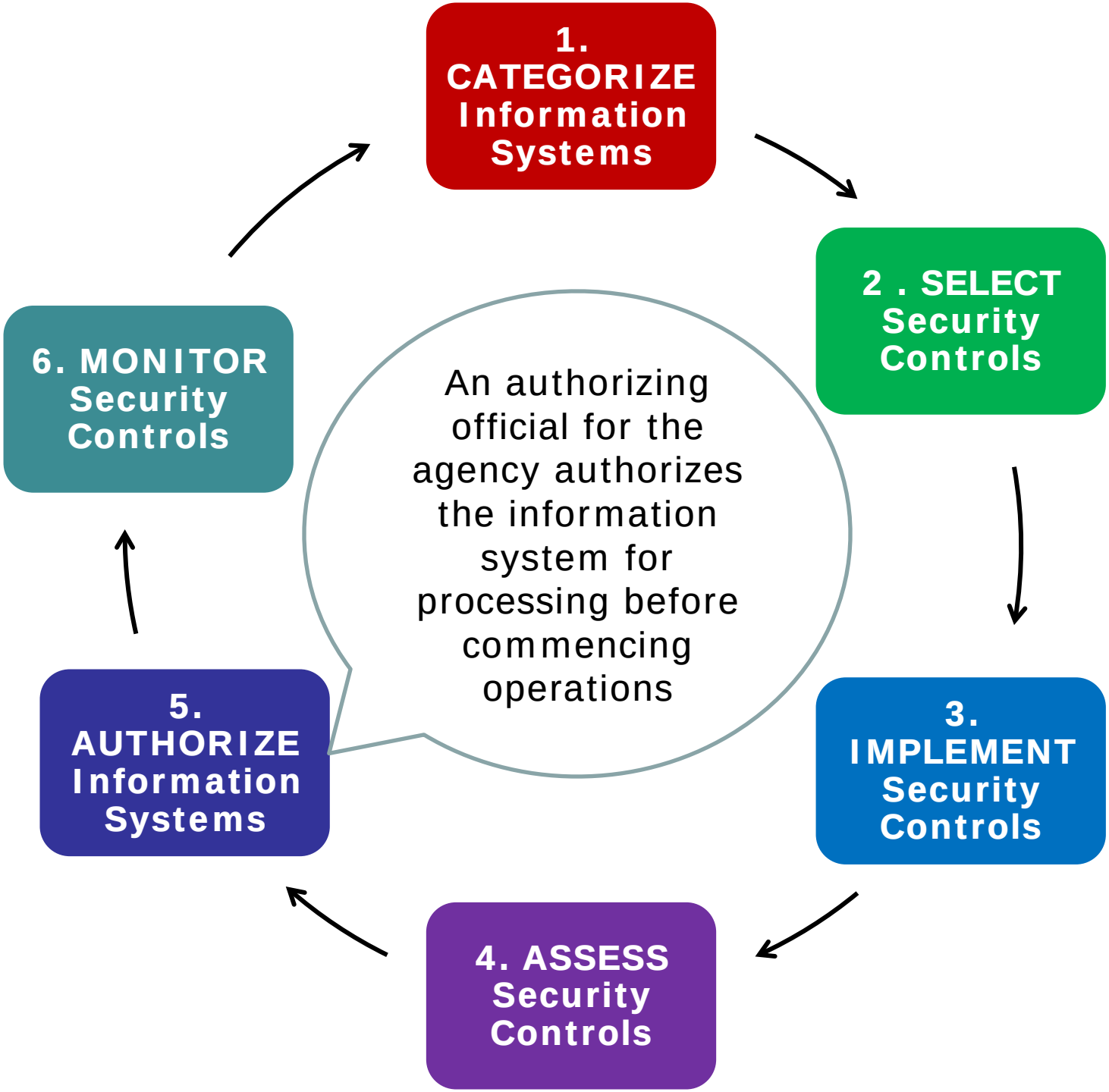

1. CATEGORIZE Information Systems
2 . SELECT Security Controls
3. IMPLEMENT Security Controls
4. ASSESS Security Controls
5. AUTHORIZE Information Systems
6. MONITOR Security Controls
Information Systems Security Life Cycle

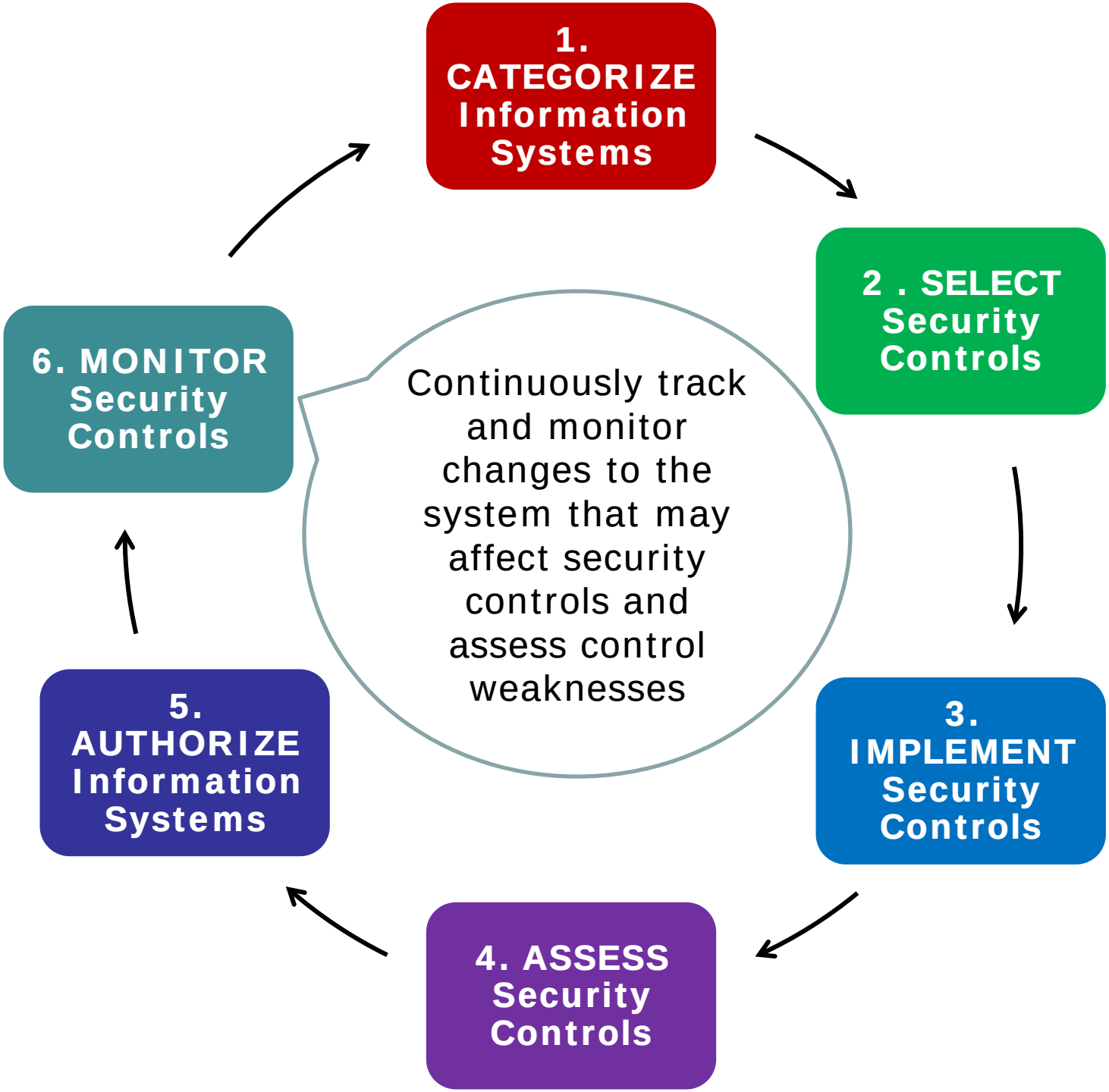

1. CATEGORIZE Information Systems
2 . SELECT Security Controls
3. IMPLEMENT Security Controls
4. ASSESS Security Controls
5. AUTHORIZE Information Systems
6. MONITOR Security Controls
Categorize & classify the system using inputs from your BIA, laws, directives, policies, strategic goals, requirements, system boundaries & resource availability

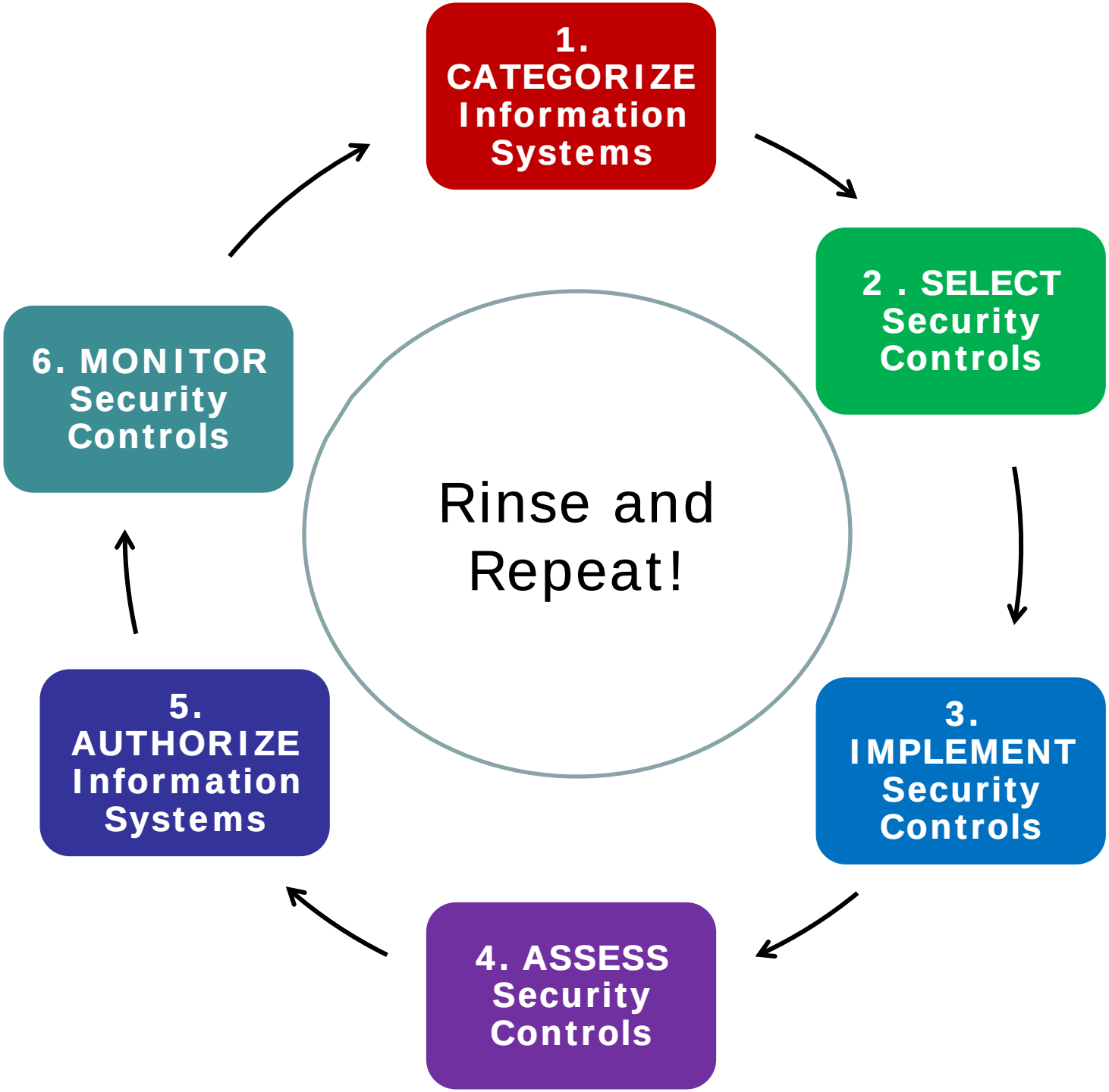

1. CATEGORIZE Information Systems
2 . SELECT Security Controls
3. IMPLEMENT Security Controls
4. ASSESS Security Controls
5. AUTHORIZE Information Systems
6. MONITOR Security Controls
Select the initial set of baseline security controls, safeguards, & countermeasures planned or in place to protect the information system


1. CATEGORIZE Information Systems
2 . SELECT Security Controls
3. IMPLEMENT Security Controls
4. ASSESS Security Controls
5. AUTHORIZE Information Systems
6. MONITOR Security Controls
Implement security controls & requirements in new or legacy information systems; implement security configuration checklists/baseline


1. CATEGORIZE Information Systems
2 . SELECT Security Controls
3. IMPLEMENT Security Controls
4. ASSESS Security Controls
5. AUTHORIZE Information Systems
6. MONITOR Security Controls
Determine the extent to which the security controls are: implemented correctly, operating as intended, & producing desired outcome


1. CATEGORIZE Information Systems
2 . SELECT Security Controls
3. IMPLEMENT Security Controls
4. ASSESS Security Controls
5. AUTHORIZE Information Systems
6. MONITOR Security Controls
An authorizing official for the agency authorizes the information system for processing before commencing operations


1. CATEGORIZE Information Systems
2 . SELECT Security Controls
3. IMPLEMENT Security Controls
4. ASSESS Security Controls
5. AUTHORIZE Information Systems
6. MONITOR Security Controls
Continuously track and monitor changes to the system that may affect security controls and assess control weaknesses


1. CATEGORIZE Information Systems
2 . SELECT Security Controls
3. IMPLEMENT Security Controls
4. ASSESS Security Controls
5. AUTHORIZE Information Systems
6. MONITOR Security Controls
Rinse and Repeat!

What is a security control?

- As defined by NIST SP 800-53:

- *"...the management, operational, and technical* ***safeguards or countermeasures*** *prescribed for an information system to adequately protect the* ***confidentiality, integrity, and availability*** *of the system and the information it contains."*

Security Controls

- Security controls (management, operational and technical) include:
  - Policies, Plans and Procedures;
  - Processes and Activities;
  - Mechanisms (hardware, software, firmware); and
  - Products and Services.

- Adequate information system security depends on security controls functioning as planned when configured, integrated, and used in the end-user operational environment.

- Accordingly, NIST 800-53 places a lot of emphasis on continuously monitoring & assessing the effectiveness of security controls.

Security Control Classes

- **Managerial—** Security controls that focus on the management of risk and the management of information system security (example: Risk Assessment)
- **Operational—** Security controls that primarily are implemented and executed by people (example: Personnel Security)
- **Technical—** Security controls that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. (example: Audit and Accountability)

Families

- Security controls in NIST 800-53 and in the new SEC 501-07 are arranged into "**families**".

- Security "families" are similar to the security "domains" we are familiar with from SEC501-06. There are 17 families included in the new SEC501-07.

Security Control Families

- Each security control family contains security controls related to the security functionality of the family.
- A **two-character identifier** is assigned to uniquely identify each security control family.
- In addition, there are three general classes of security controls: management, operational, and technical.
- The following table summarizes these relationships:

ID	FAMILY	CLASS	# Controls (nist/cov)
AC	Access Control	Technical	22/22
AT	Awareness and Training	Operational	5/5
AU	Audit and Accountability	Technical	14/9
CA	Security Assessment & Authorization	Management	7/4
CM	Configuration Management	Operational	9/9
CP	Contingency Planning	Operational	10/9
IA	Identification and Authorization	Technical	8/7
IR	Incident Response	Operational	8/8
MA	Maintenance	Operational	6/3
MP	Media Protection	Operational	6/5
PE	Physical and Environ Protection	Operational	19/13
PL	Planning	Management	6/4
PS	Personnel Security	Operational	8/7
RA	Risk Assessment	Management	5/4
SA	Systems and Services Acquisition	Management	14/10
SC	Systems & Comm Protection	Technical	34/15
SI	System and Information Integrity	Operational	13/8

Structure of a Security Control in SEC501-07

- To identify each security control, a numeric identifier is appended to the family identifier to indicate the number of the control within the family. For example, CP-9 is the ninth control in the Contingency Planning (CP) family and AC-2 is the second control in the Access Control (AC) family.

- SEC501-07 documents each security control in a **common structure** consisting of the following components: (i) a *control section; (ii) a supplemental guidance section; (iii) a control enhancements section for sensitive systems; and (iv) a references section.*

IR-2 INCIDENT RESPONSE TRAINING

Control: The organization:

a. Trains personnel in their incident response roles an to the information system; and

b. Provides refresher training *at least once ar or wh procedures are modified.*

Supplem sponse training in identifi cious activities sources

Control E e Systems:

(1) The organ on s into incident response training to facilitate ective sis situations.

(2) *[Withdrawn: N*

Previous COV ITRM SEC 501-06 Control References: 8.3.2.3

The **control** statement de rela be or b

The **supplemental guidance** section provides additional information related to a specific security control, but contains no requirements. Agencies are expected to apply the supplemental guidance as appropriate, when defining, developing, & implementing security

The **control enhancements for sensitive systems** section provides statements of security capability to: (i) build in additional functionality to a control; and/or (ii) increase the strength of a control.

You will also see **Withdrawn** controls. These are NIST controls that we will not be implementing as SEC501-07 controls at this time.

The **previous references** section provides a mapping back to the control # used in the previous version SEC501-06.

You will also see controls with a **COV** extension. These controls are not part of NIST 800-53 but have been added to SEC501-07 to assure compliance with § 2.2-2009 and other Commonwealth laws or regulations.

IR-4- COV

Control:

1. Identify immediate mitigation procedures, including specific instructions, based on information security incident categorization level, on whether or not to shut down or disconnect affected IT systems.

2. Establish procedures for information security incident investigation, preservation of evidence, and forensic analysis.

Supplemental Guidance: None

Control Enhancements for Sensitive Systems: None

Previous COV ITRM SEC 501-06 Control References: 9.4.2

Virginia Information Technologies Agency

APPENDIX B – SEC 501-06 to SEC 501-07 Control Reference

Use Appendix B to crosswalk requirements referenced in SEC501-06 to requirements in the new SEC501-07.

8.3.2 Requirements	Each agency ISO shall:	Ref #
1	Include any Agency-specific training requirements in the Agency information security awareness and training program.	AT-2
2	Require that all IT system users, including employees and contractors, receive IT security awareness training annually, or more often as necessary. Generally, best practice is that annual security awareness training lasts at least one hour.	AT-2
3	Require additional role-based information security training commensurate with the level of expertise required for those employees and contractors who manage, administer, operate, and design IT systems, as practicable and necessary.	AT-3

Helpful NIST Publications

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Assessment)
- NIST Special Publication 800-39 (Risk Management)
- NIST Special Publication 800-37 (Certification & Accreditation)
- NIST Special Publication 800-53 (Recommended Security Controls)
- NIST Special Publication 800-53A (Security Control Assessment)
- NIST Special Publication 800-60 (Security Category Mapping)

- Many others: http://csrc.nist.gov/publications/PubsSPs.html

Summary

- **Agency education**: For the next few months at ISOAG, CSRM will continue to present more information about SEC 501-07.

- We'll be discussing many of the specifics about what's included in many of the security control families.

- We are also in the process of developing new policies, guidelines, & templates to help support agencies as we move towards full implementation of the new standard.

When does this happen?

- Effective Date: We expect SEC501-07 to be effective October 1, 2012.

- Compliance Date: We'll target compliance with the new standard for January 1, 2013.

Questions

Virginia Information Technologies Agency

Cyber Security Month

October 2012

Ed Miller
Security Analyst

"Cybersecurity is not an end unto itself; it is instead an obligation that our governments and societies must take on willingly, to ensure that innovation continues to flourish, drive markets, and improve lives."

-- President Barack Obama

Research Findings

- 96 % of Americans feel a personal responsibility to be safer and more secure online.
- 93 % believe their online actions can protect not only friends and family but also help to make the Web safer for everyone around the world.
- 61 % believe that much of online safety and security falls under their personal control.
- 90 % said they want to learn more about keeping safer on the Internet.

Research Findings

- 48 % feel their actions to stay safe and secure can have a positive impact on financial, economic, and national security of the country.

- 54 % are extremely concerned about loss of personal or financial information.
- Compare that to:
  - 53 % concerned about losing their jobs
  - 51 % feared not being able to provide healthcare for their family

- 67% of the American public have heard, read or seen something about online safety and security issues recently.

Research Findings

- 28% say they lacked the information or knowledge of the things they can or should do to stay safer online.
- 12% said online safety was too expensive.
- 5% said they were too busy to take the extra step.
- *Heart + Mind Strategies conducted this national survey online with 1,007 U.S. adults ages 18 and up between May 21-25, 2010.*

Cyber Security Awareness Month

October is National Cyber Security Awareness Month (NCSAM).

NCSAM has been conducted every October since 2001. It is sponsored by the Department of Homeland Security in cooperation with the National Cyber Security Alliance (NCSA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC).

What is Cyber Security Awareness?

The Oxford English Dictionary defines **awareness** as "The quality or state of being aware; consciousness." **Aware** is defined as "Informed; cognizant; conscious; sensible."

The purpose of cyber security awareness presentations is simply to focus attention on cyber security.

Awareness presentations are intended to allow individuals to recognize information technology security concerns and respond accordingly.

Why is Cyber Security Awareness Important?

To protect the confidentiality, integrity, and availability of information in the Commonwealth requires that all employees:

- Understand their roles and responsibilities related to the Commonwealth and agency mission
- Understand the Commonwealth & the agency's information technology security policy, procedures, and practices
- Have at least adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible

Why is Cyber Security Awareness Important?

- Cyber security awareness programs impress upon users the importance of cyber security and the adverse consequences of its failure.

- “Awareness” may sometimes just reinforce knowledge that is already gained, but over time & with enough repetition, awareness can produce security behaviors that are automatic.

- The goal is to make "thinking security" a natural reflex for everyone in the Commonwealth. Awareness activities can build in these reflexes both for the security professional and for the everyday user.

How and where do we start?

- Getting ready for National Cyber Security Awareness Month takes a little planning and some effort.

- Here's a "How To…" that I found. It has the steps to take in planning for NCSAM. You might find these helpful.

How to plan for NCSAM?

1. **What cyber security awareness needs does your agency have?**

   How cyber security savvy are your employees already?

   Are there certain types of incidents, compromises, or support issues that are occurring frequently?

   What are the messages you want to emphasize? Which needs are most critical?

How to plan for NCSAM?

2. **Who is your targeted audience?**

Will your awareness efforts be aimed at the entire agency or just a subset (employees, citizens, executives, IT admins, etc.)?

Another way to identify your audience is to think about who in the agency most needs to hear about computer security threats & how to protect against them. Does one group of users pose more of a security risk to your information technology environment than another group?

How to plan for NCSAM?

3. **Is your intended audience in one geographic area, or dispersed?**

One geographic location would allow for events such as a security fair or invited speakers, while dispersed locations may require a strategy involving e-mailings or publications instead.

How to plan for NCSAM?

4. **What types of awareness methods tend to work in your agency?**

For some agencies, a speaker series might draw a large % of the audience & be most effective. In others, email tips and alerts may have the most impact.

Consider what methods of communication work best in your environment. What has been successful in the past? Which methods capture the attention of the most people?

How to plan for NCSAM?

4 (continued). **What types of awareness methods tend to work in your agency?**

Some examples include:

Book Marks	**Pamphlets**
Brochures	**Links Security Web Page(s)**
Checklists	**Videos**
Flyers	**Security Awareness Documents**
Games	**Security Cards**
Handouts	**Security Quizzes**
Post Cards	**Surveys**
Presentations	**Security Tools**

How to plan for NCSAM?

5. **How much money do you have to spend?**

Your budget will influence many of your decisions, and usually this is not much. However, there are many inexpensive and free resources you can utilize.

How to plan for NCSAM?

6. **How many people are available to assist?**

How many staff from your agency can assist with this effort? Can you solicit volunteers, interns, and partnerships with other divisions or units?

Remember that this doesn't have to be strictly an IT security effort. HR, Finance, Admin, Communications & many other business units within a typical agency are all stakeholders that benefit from a successful cyber security campaign.

How to plan for NCSAM?

7. **How much lead time do you have?**

National Cybersecurity Awareness Month is October.

Make sure you have enough lead time to take on the things you want to do. Consider print time and delivery time if you want to create printed material.

The more lead time you have the better. However, if you have little lead time, don't give up! There are many resources available that you can pull together quickly.

Resources

Resources: Web links

- http://www.stopthinkconnect.org/
- http://www.staysafeonline.org
- http://www.microsoft.com/security
- http://www.dhs.gov/national-cyber-security-awareness-month
- http://msisac.cisecurity.org/
- http://onguardonline.gov
- http://protect.iu.edu/cybersecurity/downloads

Resources: Blogs

- **Check out these blogs to learn more ways to protect yourself and help keep the web a safer place for everyone.**
  - Facebook Security Blog
  - Google Online Security Blog
  - Krebs on Security
  - McAfee Family Safety Blog
  - Microsoft Security Tips & Talk Blog
  - RSA Speaking of Security Blog
  - Sophos Naked Security Blog
  - Stay Safe Online Blog
  - Symantec Security Blogs
  - The Security Skeptic
  - U.S. Department of Homeland Security Cybersecurity Blog
  - Visa Security Sense Blog

Resources: TWITTER

- How to Get Involved with National Cyber Security Awareness Month Twitter Chat *Twitter*

- Sep 20 - 21, 2012

  – Join STOP. THINK. CONNECT., The National Cyber Security Alliance and the Multi-State Information Sharing Analysis Center as we gear up for National Cyber Security Awareness Month in October. Learn easy ways to get involved and make a difference in your home, school, office and community. **When:** Thursday, Sept. 20, 2012 at 3 p.m. ET/noon PT

- **Guests:** The National Cyber Security Alliance (@StaySafeOnline), MS-ISAC/Center for Internet Security (@CISecurity)
- **RSVP:** http://chatstcseptember202012.eventbrite.com/
- Use the hashtag #ChatSTC to join the conversation!

Resources: Social Media Safety

- Facebook/SaferOnline
- Twitter/SaferOnline
- YouTube/MSFTOnlineSafety

Resources: Free Checkups

- Many computer security vendors offer free computer security checks for computers. The links below are useful for employee home computers to check for known viruses, spyware, and to discover if the computer is vulnerable to cyber attacks.

AOL Computer Checkup
Audit My PC
Bitdefender
ESET Online Scanner
Kaspersky Virus Scanner
McAfee Security Scan
Microsoft Safety Scanner
nCircle PureCloud Vuln. Scanner

Norton Security Scan
Panda Security Antivirus Scan
Qualys Browser Check
QualysGuard Malware Protection
Secunia PSI
Sophos Free Security Tools
Symantec Security Scan
Trend Micro HouseCall Virus Scan
Webroot Secure Anywhere Antivirus

Resources: NIST HIPAA Security Toolkit

- The NIST HIPAA Security Toolkit Application is intended to help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environment.

- http://scap.nist.gov/hipaa/

Virginia Information Technologies Agency

Resources: UVA

ISPRO
Information Security, Policy, and Records Office

- University of Virginia, Newcomb Hall, Kaleidoscope Room
- Oct 2 - 26, 2012
  - Attend one of four security awareness presentations for National Cybersecurity Awareness Month, hosted by the **University of Virginia Information Security, Policy, and Records Office (ISPRO)**.
  - Learn how to protect your data, identity, and computers from the ever-intrusive spread of malware by attending one of these security awareness presentations.
  - October 02, 2012 — 1:30 - 2:30PM
  - October 08, 2012 — 11:00AM - 12:00PM
  - October 17, 2012 — 12:30 - 1:30PM
  - October 25, 2012 — 11:30AM - 12:30PM

Win Door prizes!

Virginia Information Technologi

COV Resources

Many Commonwealth ISOs and auditors are experts in a number of IT security areas & are always willing to help or share their knowledge.

PROFES

Developing Security Education and Awareness Programs

Prevention in the form of education and awareness programs can help campuses avoid serious security ills

By **Shirley Payne**

"Grad Student Charged with Hacking"
"Security Lapses Permit Theft from Database"
"Student Is Charged in Theft of Social Security Numbers"
"Campus Network Administrators Say Timing of Sobig.F Virus Couldn't Have Been Worse"

The Case for Security Education

First, let's talk about why a security education and awareness program is so important—even when putting it together takes a lot of time and energy. Experts generally agree that people are the greatest source of IT security problems. Statistics consistently show that

- few computer users acknowledge personal responsibility for security,
- many consider the issue too technically complex for them to understand,
- executives and middle managers often fail to comprehend the business implications of poor security and consequently don't assign it a high pri-

Virginia Information Technologies Agency

Resources: Posters / Calendars

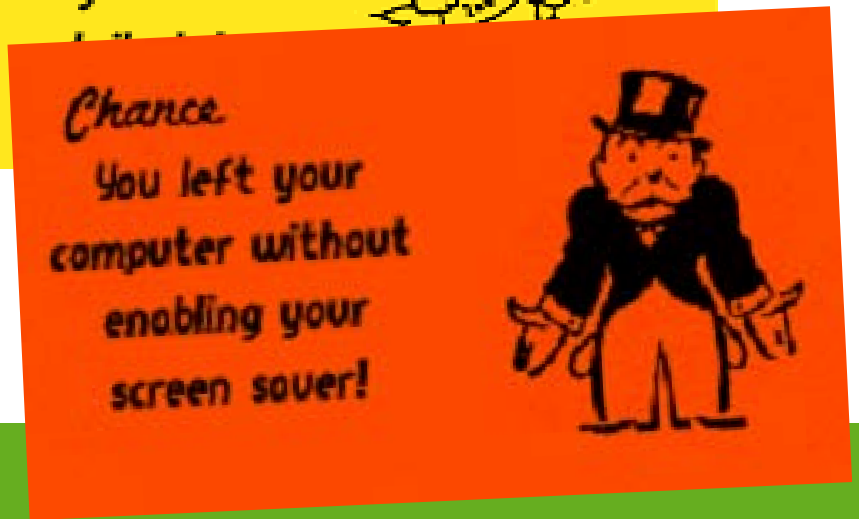
- VITA has loads of posters, calendars, and bookmarks that promote cyber security in various ways. We seem to always have way more than we can get rid of. Please take all you want.

Virginia Information Technologies Age

http://www.signgenerator.org/games/monopoly/

Resources: Let them know

- If you catch them doing some wrong, let them know so they can fix it. If you catch them doing some right, let them know so they'll continue to do it.



Resources: Quizzes, Games, Videos

Onguardonline.gov (sponsored by the FTC)

Cyber Security Month at VITA

- At VITA, we try to do a little extra something every year for our employees to promote Cyber Security Month.

- We encourage all agencies to try to promote it within their organization as well.

Planning your message

- Generally, it is more effective to identify one or a few focused messages and repeat those many times rather than to try to be very general.

- Consider focusing on one message/topic per each week in October, or one message/topic for the entire month with sub-topics each week.

Areas of Focus (example agenda)

- Week 1: Secure Social Media
- Week 2: Mobile Device Security
- Week 3: Computer Security While Traveling
- Week 4: Privacy of Information
- Week 5: Employee Participation Game

Sample Cyber Security Month Agenda

- Each Monday: a Security Buzz (a security email tip related to the focus of the week)
- Each Wednesday: a link to a Security Quiz, Video or Game
- Each Friday: a security crossword or word search puzzle (also related to the security focus of the week).
- October 17: Cyber Security Day at VITA (Keynote speaker)

Let us know

- Finally, we are interested in the efforts that you've made at your agency in promoting cyber security awareness.

- If you have powerpoint presentations, posters, tips, speaker sources, that you'd be willing to share, please let us know.

- Remember, October is just the peak month. A successful cyber security awareness campaign really needs to run all year long.

Ed Miller

VITA
Commonwealth Security and Risk Management
edward.miller@vita.virginia.gov
(804)-416-6027

Upcoming Events

Governor's Proclamation

Governor McDonnell has proclaimed
October 2012
as
Cyber Security Awareness Month

Proclamation will be located at the Governor's Portal:
http://www.governor.virginia.gov/OurCommonwealth/Proclamations/

or VITA Information Security Awareness Toolkit:
http://www.vita.virginia.gov/security/toolkit/default.aspx?id=9930

Virginia Information Technologies Agency

COVITS 2012

COVITS is a forum to discuss technology requirements, share valuable lessons from actual case studies, and glimpse the future of government interaction with its customers.

September 6 & 7

Hilton Richmond Hotel @ Short Pump

12042 West Broad Street, Richmond, VA 23233

Register Here: https://events.govtech.com/events/covits2012/reg

Virginia Information Technologies Agency

Center for Internet Security Buy Opportunity

Center for Internet Security's Trusted Purchasing Alliance Division

- The Alliance is pleased to announce that NetLib will be offering all state, local, education and nonprofit organizations a 78% discount on their NetLibEncryptionizer for SQL databases.
- **Buy period runs from August 17 to October 31.**
- Refer to email sent 8/27 from Commonwealth Security for Buy Pricing specifics.

OR

Contact:

The Center for Internet Security/Trusted Purchasing Alliance at info@cisalliance.org

Jessica Williams at (518)266-3460

Virginia Information Technologies Agency

COV Training: Creative Thinking for Auditors

DATE: Sept 11 & 12, 2012

LOCATION: DOE Conference Room on 22nd Floor
James Monroe Building
101 North 14th Street, Richmond, VA 23233

TIME: 8:15a - 4:45p.

COST: $160/day or $320/class
16 CPEs will be awarded for class

Trainer: Carole Buncher

Register: https://hrtraining.doa.virginia.gov

Contact: Tim Sadler (804)225-3106 x 23 or tim.sadler@doa.virginia.gov with any questions

Virginia Information Technologies Agency

Information Security System Association

ISSA

DATE: Wednesday, Sept 12, 2012

LOCATION: Maggiano's Little Italy
11800 West Broad Street, #2204, Richmond, VA 23233
TIME: 11:30 - 1:00pm. Presentation starts at 11:45.
Lunch served at 12.
COST: ISSA Members: $20 & Non-Members: $25

SPEAKER: Kabir Mulchandani (Managing Principal at **Cigital)**

TOPIC: ***Developing a Software Security Assurance Program***

Virginia Information Technologies Agency

ISSA Central VA Chapter: CISSP Study Group

DATE: Tuesdays, Sept 25 thru Dec 18, 2012

TIME: 6:00 - 9:00pm.
LOCATION: VCU Computer Center aka "The UCC"
Pocahontas Building
900 East Main Street, Richmond, VA 23233
COST: $450 includes pizza & soft drinks
MUST be an ISSA Central VA Chapter member!!
*** NO Exceptions**

For further details & registration:
http://centva.issa.org/training/

Virginia Information Technologies Agency

MS-ISAC

National Webcast Initiative

Thursday, Oct 11

2:00 pm – 3:00 pm EDT

Topic: **Cyber Security: What you should know to stay safe online**

Visit MS-ISAC web for more information:

http://www.msisac.org/webcast/

Future ISOAG Dates

Oct 3	1:00 – 4:00 pm @ CESC
Nov 7	1:00 – 4:00 pm @ CESC
Dec 5	1:00 – 4:00 pm @ CESC

ISOAG will be held the 1st Wednesday of each month in 2012

IS Orientation Sessions

Tuesday - Nov 13, 2012 9:00 – 11:30a (CESC)

Email CommonwealthSecurity@VITA.virginia.gov if you are interested in attending.

IS Orientation also available via webinar!

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**

ISOAG-Partnership Update

IT Infrastructure Partnership Team
Bob Baskette

Sep 5, 2012

ADJOURN

Source: www.pcmag.com