GreyCastle security

You Had Me at 'Compliance':

Get ready for your close-up with Federal regulations

500 Federal Street
Suite540
Troy, NY 12180
www.greycastlesecurity.com
(800) 403-8350

PRESENTER

Stephen Lau
Senior Security Specialist
GreyCastle Security
slau@greycastlesecurity.com

GreyCastle security

GOAL ONE	GOAL TWO	GOAL THREE
Understand the difference between security and compliance.	Awareness of the complex Federal regulatory environment.	Awareness of standards and paths forward.

GreyCastle

SECURITY AND COMPLIANCE

IS THERE A DIFFERENCE?

GreyCastle
security

SECURITY AND COMPLIANCE

IS THERE A DIFFERENCE?

COMPLIANCE DOES NOT EQUAL SECURITY.

- You can be compliant and have insecure systems
- You can have secure systems and be non-compliant

GreyCastle security

SECURITY AND COMPLIANCE: FINDING A BALANCE

- Identify organization's ***risk appetite***
  - Ongoing conversation between stakeholders and leadership
- Some factors that influence risk appetite
  - Organizational structure
    - Strong governance or decentralized?
  - Available resources
  - Maturity of organization's security program
  - External / internal expectations
    - What is everyone else doing?
    - What is considered best practice?
  - Nature of the risk

GreyCastle security

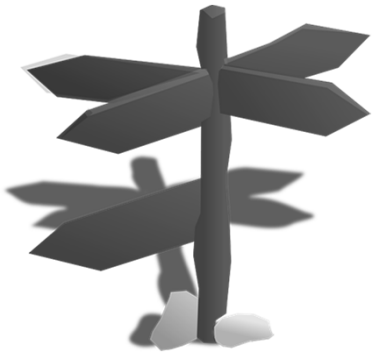
TERMS & DEFINITIONS

- **Information Security / Cybersecurity** – Used interchangeably in Federal landscape. Most Federal regulations use cybersecurity
- **Control** – Measures that modify risk (NIST SP 800-53)
  - Examples include policy, anti-virus, and physical locks
- **Compensating control** – Equivalent or comparable protection for an information system. (NIST SP 800-53)
- **Nonconformity** – Misalignment between regulation or standard and practice or documentation
- **Corrective action / Plan of action and milestones (POA&M)** – Activity to address a nonconformity

GreyCastle security

FEDERAL REGULATORY LANDSCAPE

- Regulations lag behind technology
  - Often focused on threat du jour (d'hier)
- Can be contradictory or vague
  - Often created by non-technologists
- Complex
  - Approximately 900 NIST SP 800-53 controls
- Moving toward a risk-based approach
  - Increases flexibility for security
  - Increases complexity for compliance
  - Less checkbox security / More "explain why"



GreyCastle security

(SOME) FEDERAL STANDARDS AND REGULATIONS

- Federal Information Management Security Management Act / Federal Information Processing Standards (FISMA / FIPS)
- National Institute of Standards and Technology (NIST) Risk Management Framework
- NIST Cybersecurity Framework
  - Uses risk management to address cybersecurity
- Federal Risk and Authorization Management Program (FedRAMP)
  - Addresses cybersecurity for cloud services

GreyCastle security

FISMA / FIPS

- Developed in 2002 (reformed in 2014) by Federal government
  - Often used and abused
- Applicable to:
  - Federal systems
  - State agencies administrating Federal programs
  - Private companies with Federal contracts
- Related documents.
  - FIPS 199 – System categorization - High / Medium / Low
  - FIPS 200 – Minimum security requirements
  - NIST SP 800-53 Revision 4 – Catalog of security controls

GreyCastle security

NIST SPECIAL PUBLICATION 800-53 Rev 4

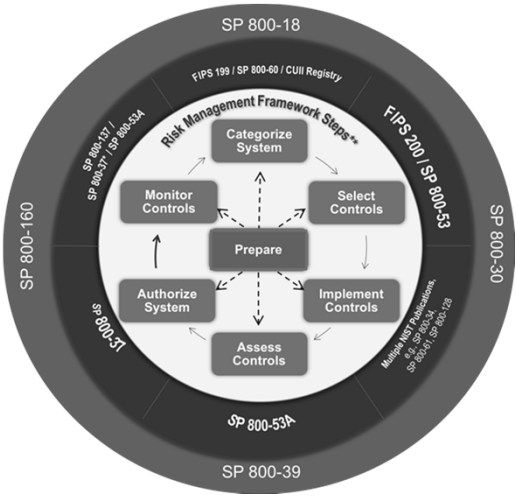
- Catalog of security controls broken up into 18 ***control families***
  - 3 Baselines (Low / Medium / High)
  - Each control family has ***control enhancements***

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational

Identifier	Family	Class
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Service Acquisition	Management
SC	System and Communication Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

GreyCastle security

NIST RISK MANAGEMENT FRAMEWORK



GreyCastle security

METHODS TO ADDRESS RISK

- Avoid
  - Don't do whatever it is that causes the risk
- Mitigate
  - Implement a control to modify / reduce the risk
- Transfer
  - Transfer the risk to a third party
  - Examples: Obtain insurance or outsource the activity (e.g. cloud)
- Accept
  - When the cost to mitigate the risk outweighs the benefit
  - Often used in risks associated with outdated technology or a low risk probability

Addressing risk does not necessarily mean eliminating risk!

GreyCastle security

NIST CYBERSECURITY FRAMEWORK

- Originally published in 2014
  - Targeted for operators of critical infrastructure
- Effort to further shift towards risk management based cybersecurity
- 5 functions and 22 categories
  - Each category has subcategories or outcomes and controls
  - 98 subcategories

GreyCastle security

NIST CYBERSECURITY FRAMEWORK

GreyCastle security

OTHER STANDARDS AND REGULATIONS

- Industry specific standards
  - NERC CIP Cybersecurity Standards
- Internationally accepted standards
  - ISO/IEC 27001:2013
  - Center for Internet Security (CIS) Critical Security Controls

Not an exhaustive list – Your mileage will vary.

GreyCastle security

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION (NERC)

- 2006 - Federal Energy Regulatory Commission (FERC) designated NERC to be the United States Electric Reliability Organization (ERO)
- NERC Critical Infrastructure Protection (CIP)
  - 11 standards with controls.

Name	Title
CIP-002-5.1a	BES Cyber Security Categorization
CIP-003-6	Security Management Controls
CIP-004-6	Personnel & Training
CIP-005-5	Electronic Security Perimeter(s)
CIP-006-6	Physical Security of BES Cyber Systems
CIP-007-6	System Security Management
CIP-008-5	Incident Reporting and Response Planning
CIP-009-6	Recovery Plans for BES Cyber Systems
CIP-010-2	Configuration Change Management and Vulnerability Assessments
CIP-011-2	Information Protection
CIP-014-2	Physical Security

GreyCastle security

ISO / IEC 27001 INFORMATION SECURITY MANAGEMENT

- International standard
- Focuses on governance and process vs. specific technologies
  - Information Security Management System (ISMS)
- Attempts to achieve a more wholistic approach to information security
  - Information security and risk decisions at the organizational level
  - Reduces silo effects
- 10 Mandatory Clauses + Annex of 18 controls

GreyCastle security

CENTER FOR INTERNET SECURITY (CIS) CRITICAL SECURITY CONTROLS

- Originally developed by SANS Institute
  - SANS Top 20 Security Controls
- Focuses on controls
  - Risk is based upon historical incidents and situations analyzed by CIS and SANS
- Controls are least common denominator

GreyCastle security

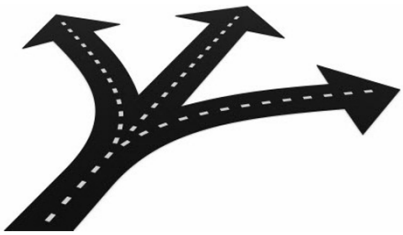
CENTER FOR INTERNET SECURITY (CIS) CRITICAL SECURITY CONTROLS

Name	Title
CSC 1	Inventory of authorized and unauthorized devices
CSC 2	Inventory of authorized and unauthorized software
CSC 3	Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers
CSC 4	Continuous vulnerability assessment and remediation
CSC 5	Controlled use of administrative privileges
CSC 6	Maintenance, monitoring, and analysis of audit logs
CSC 7	Email and web browser protections
CSC 8	Malware defenses
CSC 9	Limitation and control of network ports, protocols, and services
CSC 10	Data recovery capability
CSC 11	Secure configurations for network devices such as firewalls, routers, and switches
CSC 12	Boundary defense
CSC 13	Data protection
CSC 14	Controlled access based on the need to know
CSC 15	Wireless access control
CSC 16	Account monitoring and control
CSC 17	Security skills assessment and appropriate training to fill gaps
CSC 18	Application software security
CSC 19	Incident response and management
CSC 20	Penetration tests and red team exercises

GreyCastle security

WHERE TO FROM HERE?

- Most of standards overlap each other
  - You may be required to comply with one or more standards
  - Pick a path and justify it
  - Identify mappings
- Develop a risk based approach to information security and compliance
- Compliance becomes more difficult to identify and document



GreyCastle security

RISK BASED SECURITY AND COMPLIANCE

- Less focus on the technology (how)
- Address the actual risks and threats
  - Minimize paper tiger threats
- Risk decisions made at the organizational level
  - Can be difficult with decentralized organizations
- Address risk with controls
  - Avoid / mitigate / transfer / accept

GreyCastle security

RISK BASED APPROACH TO COMPLIANCE

- Perform and document an annual quantitative risk / gap assessment.
  - Those doing should not be the ones assessing
  - More conversational / less check-boxing
- Identify risks that fall above your organization's risk acceptance criterion
  - Your organization's risk acceptance criterion may initially be high
- Risks that fall above your risk acceptance criterion should be Corrective Actions / POA&Ms

GreyCastle security

COMPENSATING CONTROLS

- Equivalent or comparable protection for an information system. (NIST SP 800-53)
- Most standards have flexibility in "how"
  - Use this flexibility along with risk management to address gaps
- Document and gain approval of rationale
  - Did I mention document?
- Example compensating control:
  - Encryption of databases – can be expensive and operationally problematic
  - Compensating controls: Extensive logging of access, tighter access requirements, data loss prevention monitoring

GreyCastle security

CORRECTIVE ACTIONS / POA&Ms

- Track and document Corrective Actions
- Identify and assign an owner / champion
  - Hold these individuals responsible
- Identify risk treatments (avoid / mitigate / transfer / accept)
- Identify and document any compensating controls
- Assign a timeline for implementation
- Document progress of implementations and resolution (if any)
- If nothing is done, you've effectively operationally accepted the risk, at least for now

Be realistic!

GreyCastle Security

SECURITY AND COMPLIANCE ARE NOT THE SAME THING	IMPLEMENT A RISK BASED APPROACH TO SECURITY AND COMPLIANCE	BE PROACTIVE AND REALISTIC

GreyCastle Security

GreyCastle
security

QUESTIONS?

slau@greycastlesecurity.com
(800) 403-8350
www.greycastlesecurity.com