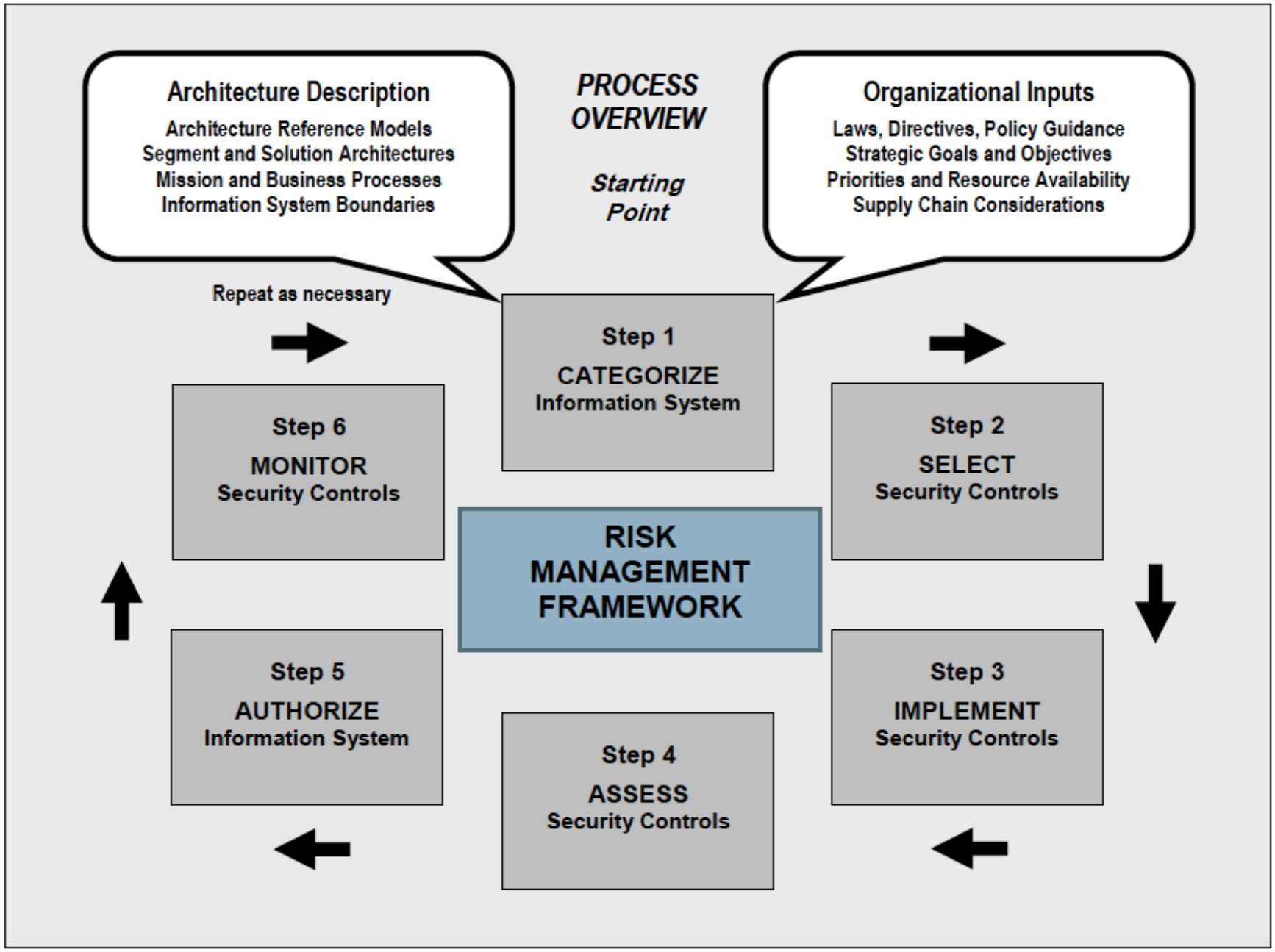
Security Controls

Chris Hankin

NIST Cyber Security Framework



From NIST sp 800-82r2

Categorisation of Systems

- Example from NIST sp 800-82r2:

- SC sensor data = {(C, NA), (I, HIGH), (A, HIGH)}
- SC admin info = {(C, LOW), (I, LOW), (A, LOW)}
- SC SCADA = {(C, LOW), (I, HIGH), (A, HIGH)}

- After re-assessment:
- SC SCADA = {(C, MODERATE), (I, HIGH), (A, HIGH)}

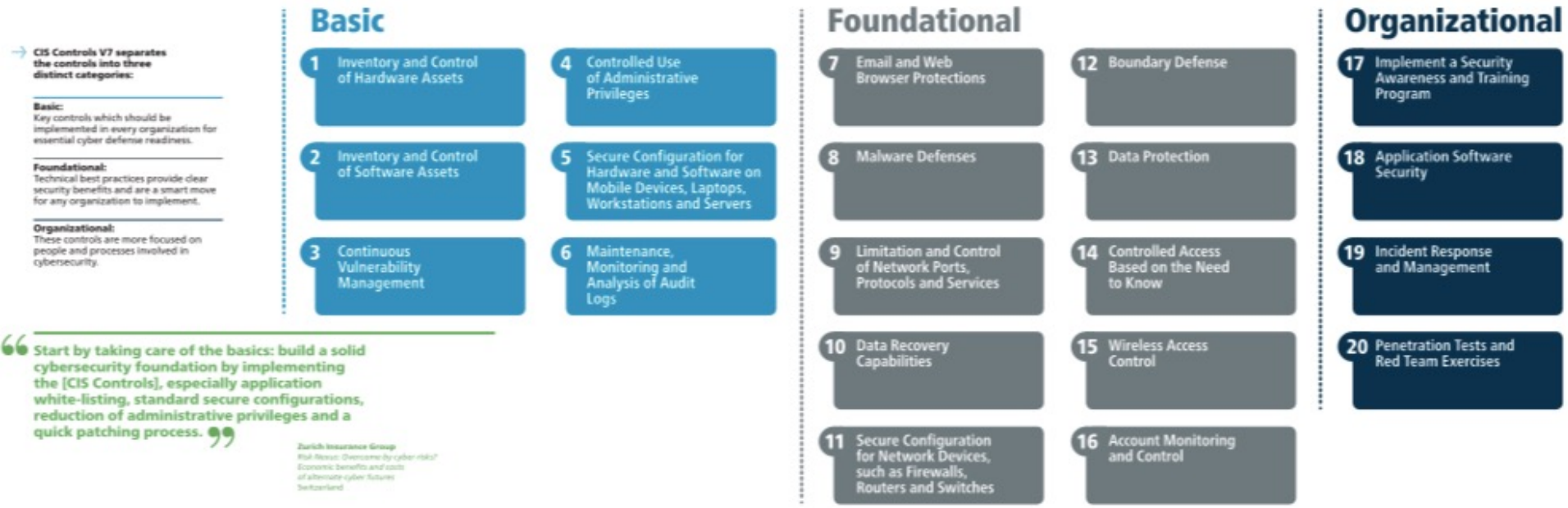
ICS Impact Levels based on ISA99

Impact Category	Low-Impact	Moderate-Impact	High-Impact
Injury	Cuts, bruises requiring first aid	Requires hospitalization	Loss of life or limb
Financial Loss	$1,000	$100,000	Millions
Environmental Release	Temporary damage	Lasting damage	Permanent damage, off-site damage
Interruption of Production	Minutes	Days	Weeks
Public Image	Temporary damage	Lasting damage	Permanent damage

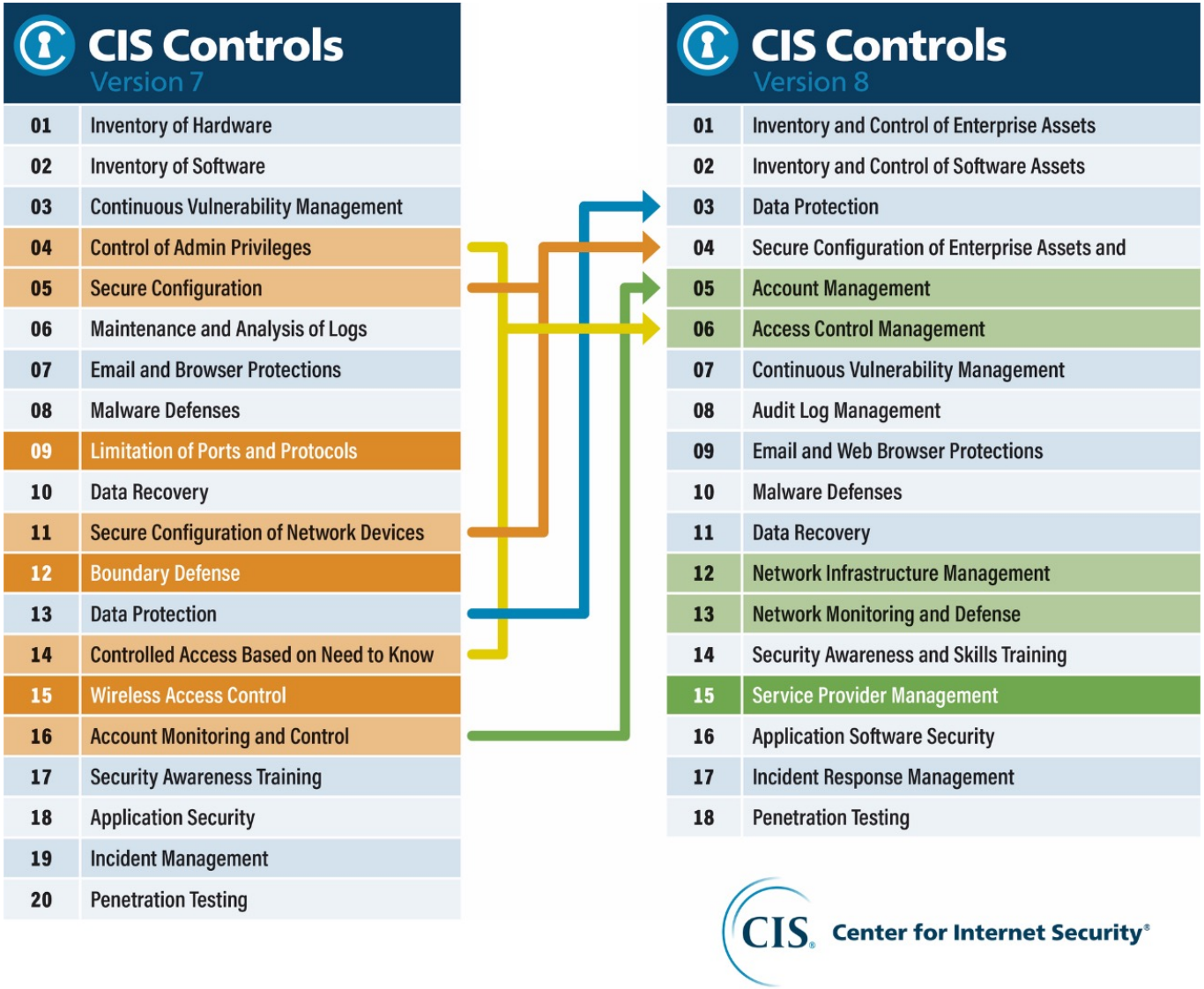
From different perspectives

Category	Low-Impact	Moderate-Impact	High-Impact
Product Produced	• Non-hazardous materials or products • Non-ingested consumer products	• Some hazardous products or steps during production • High amount of proprietary information	• Critical infrastructure (e.g., electricity) • Hazardous materials • Ingested products
Industry Examples	• Plastic injection molding • Warehouse applications	• Automotive metal industries • Pulp and paper • Semiconductors	• Utilities • Petrochemical • Food and beverage • Pharmaceutical
Security Concerns	• Protection against minor injuries • Ensuring uptime	• Protection against moderate injuries • Ensuring uptime • Capital investment	• Protection against major injuries/loss of life • Ensuring uptime • Capital investment • Trade secrets • Ensuring basic social services • Regulatory compliance

SANS Institute CIS Controls



SANS CIS Controls V8



Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

Selecting Controls (NIST sp 800-82)

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
AC-1	Access Control Policy and Procedures	**AC-1**	**AC-1**	**AC-1**
AC-2	Account Management	**AC-2**	**AC-2 (1) (2) (3) (4)**	**AC-2 (1) (2) (3) (4) (5)** (11) (12) (13)
AC-3	Access Enforcement	**AC-3**	**AC-3**	**AC-3**
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	**AC-5**	**AC-5**
AC-6	Least Privilege	Not Selected	**AC-6 (1) (2) (5) (9) (10)**	**AC-6 (1) (2) (3) (5) (9) (10)**
AC-7	Unsuccessful Logon Attempts	**AC-7**	**AC-7**	**AC-7**
AC-8	System Use Notification	**AC-8**	**AC-8**	**AC-8**
AC-10	Concurrent Session Control	Not Selected	Not Selected	**AC-10**
AC-11	Session Lock	Not Selected	**AC-11 (1)**	**AC-11 (1)**
AC-12	Session Termination	Not Selected	**AC-12**	**AC-12**
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14	AC-14
AC-17	Remote Access	**AC-17**	**AC-17 (1) (2) (3) (4)**	**AC-17 (1) (2) (3) (4)**

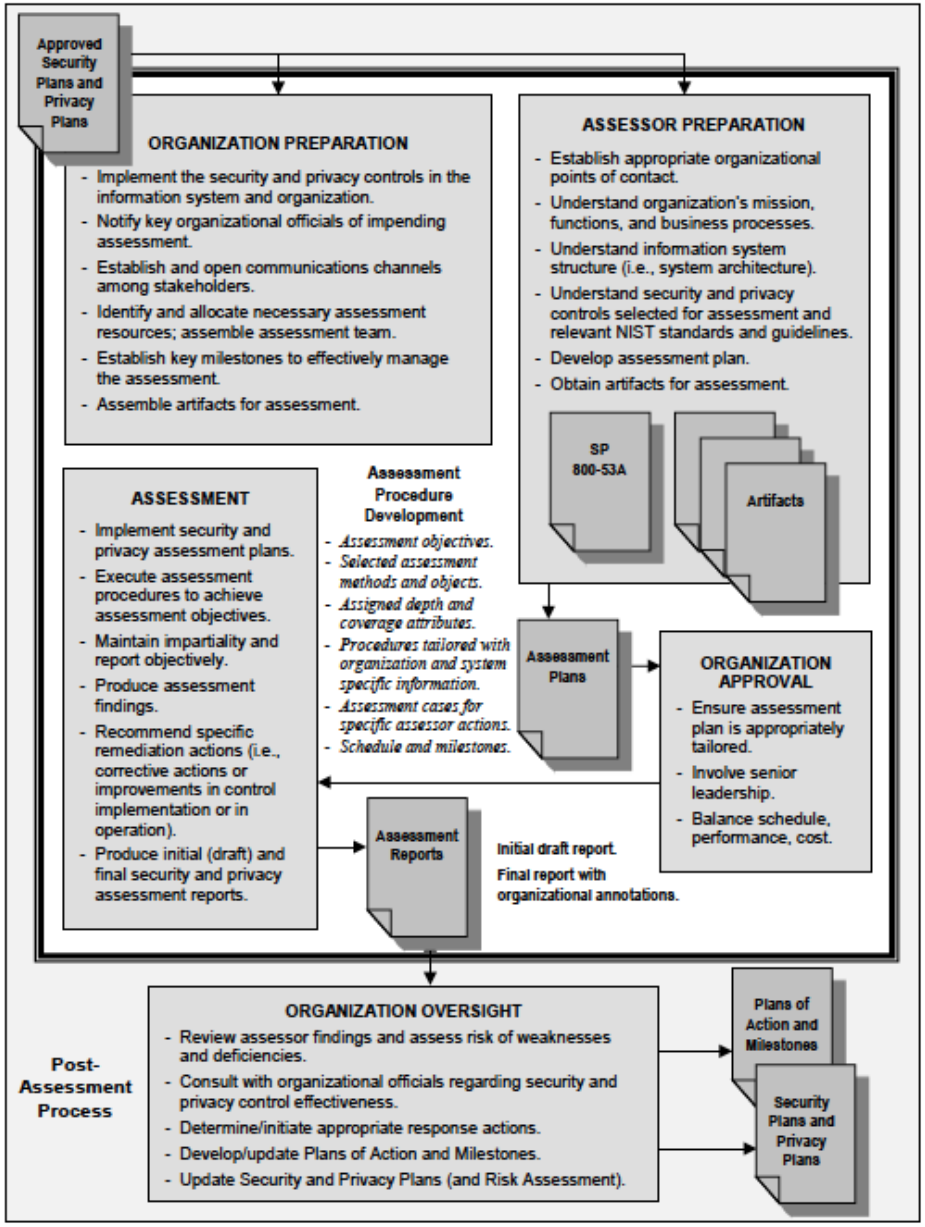
Control Enhancements

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-2	**Account Management**	**Select**	**Select**	**Select**
AC-2 (1)	*ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*		Select	Select
AC-2 (2)	*ACCOUNT MANAGEMENT | AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT*		**Select**	**Select**
AC-2 (3)	*ACCOUNT MANAGEMENT | DISABLE ACCOUNTS*		Select	Select
AC-2 (4)	*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*		Select	Select
AC-2 (5)	*ACCOUNT MANAGEMENT | INACTIVITY LOGOUT*		**Select**	**Select**
AC-2 (11)	*ACCOUNT MANAGEMENT | USAGE CONDITIONS*			Select
AC-2 (12)	*ACCOUNT MANAGEMENT | ACCOUNT MONITORING FOR ATYPICAL USAGE*			Select
AC-2 (13)	*ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS*		**Select**	**Select**

Implement Controls

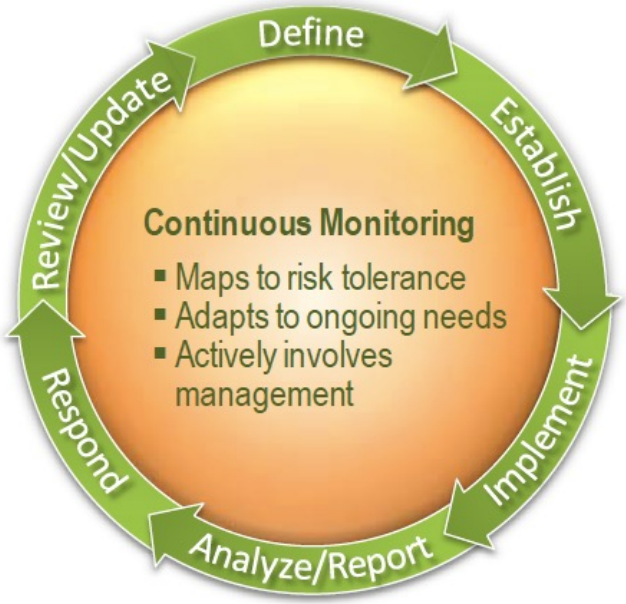
- New development: requirements definition
- Legacy: gap analysis during major upgrades, modifications or outsourcing

Assess Controls



Final Steps

- Authorize Information System
- Monitor Security Controls



Access Control

- Role-based Access (RBAC) – roles, hierarchies and constraints
- Web servers – use HTTPS where possible
- Virtual Local Area Networks (VLANs) can be used to allow switches to enforce security policies and segregation at the Ethernet layer
- Dial-up modems: use call-back if possible; change default passwords; disconnect when not in use
- Wireless – risk-based decision

Awareness and Training

- Control system specific security awareness
- Must cover the physical process as well as the ICS

- Social engineering a particular issue

- Must be monitored and documented

Audit and Accountability

- Security controls are still installed and operating correctly
- The production system is free from security compromises and provides information should they occur
- Management of change programme being followed with an audit trail
- Audit against security performance metrics

UK Cyber Assessment Framework

NIS Objectives							
A: Managing security risk		**B: Protecting against cyber attack**		**C: Detecting cyber security incidents**		**D: Minimising the impact of cyber security incidents**	
NIS Principles							
A1: Governance	A2: Risk management	B1: Service protection policies and processes	B2: Identity and access control	C1: Security monitoring	C2: Proactive security event discovery	D1: Response and recovery planning	D2: Lessons learned
A3: Asset management	A4: Supply chain	B3: Data security	B4: System security				
		B5: Resilient networks and systems	B6: Staff awareness and training				

Indicators of Good Practice

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All of the following statements are true	All the following statements are true
Your incident response plan is not documented. Your incident response plan does not include your organisation's identified essential service. Your incident response plan is not well understood by relevant staff.	Your response plan covers your essential services. Your response plan comprehensively covers scenarios that are focused on likely impacts of known and well-understood attacks only.	Your incident response plan is based on a clear understanding of the security risks to the networks and information systems supporting your essential service . Your incident response plan is comprehensive

Security Assessment and Authorisation

- Controls implemented correctly, operating as intended, and producing the desired outcome
- Senior responsible for accepting residual risk and authorizing operation
- Controls monitored on an ongoing basis

Configuration Management

- Controlling modifications to hardware, firmware, software and documentation prior to, during and after system implementation
- Controls for maintaining, monitoring and documenting configuration control changes
- There should be restricted access to configuration settings
- Security settings of IT devices should be the most restrictive consistent with ICS operational requirements

Contingency Planning

- Business Continuity Planning
  - Recovery Time Objective – time to recover comms and processing capabilities
  - Recovery Point Objective – the longest period for which the absence of data can be tolerated
- Disaster Recovery Planning

Priority Code	Sequencing	Action
Priority Code 1 (**P1**)	FIRST	Implement P1 security controls first.
Priority Code 2 (**P2**)	NEXT	Implement P2 security controls after implementation of P1 controls.
Priority Code 3 (**P3**)	LAST	Implement P3 security controls after implementation of P1 and P2 controls.
Unspecified Priority Code (**P0**)	NONE	Security control not selected in any baseline.

CP-1	Policy and Procedures	**CP-1**	**CP-1**	**CP-1**
CP-2	Contingency Plan	**CP-2**	**CP-2** (1) (3) (8)	**CP-2** (1) (2) (3) (5) (8)
CP-3	Contingency Training	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	CP-4	CP-4 (1)	CP-4 (1) **(2)**
CP-6	Alternate Storage Site		CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site		**CP-7** (1) (2) (3)	**CP-7** (1) (2) (3) (4)
CP-8	Telecommunications Services		**CP-8** (1) (2)	**CP-8** (1) (2) (3) (4)
CP-9	System Backup	CP-9	CP-9 **(1)** (8)	CP-9 **(1) (2)** (3) (5) (8)
CP-10	System Recovery and Reconstitution	**CP-10**	**CP-10** (2) **(6)**	**CP-10** (2) (4) **(6)**
CP-12	Safe Mode	CP-12	CP-12	CP-12

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-2	**Contingency Plan**	**Select**	**Select**	**Select**
CP-2 (1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*		Select	Select
CP-2 (2)	*CONTINGENCY PLAN | CAPACITY PLANNING*			Select
CP-2 (3)	*CONTINGENCY PLAN | RESUME MISSION AND BUSINESS FUNCTIONS*		Select	Select
CP-2 (5)	*CONTINGENCY PLAN | CONTINUE MISSION AND BUSINESS FUNCTIONS*			Select
CP-2 (8)	*CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*		Select	Select

Identification and Authentication

- Something you know, something you have, or something you are
- Multi-factor authentication
- Password authentication – problems in stressful situations; complexity should balance security and ease of access; avoid dictionary words and predictable sequence of integers!
- Challenge/response authentication – shared secret; possible latency issues

Identification and Authentication

- Physical token authentication
  - Traditional physical locks and keys
  - Security cards
  - Radio frequency devices in cards, key fobs, tags
  - Dongles with secure encryption keys that attach to USB or other ports
  - One-time authentication generators (key fob)
- Better used with some other authentication factor

Identification and Authentication

- Smart card authentication – additional functionality beyond physical token authentication; revocation and management of lost or damaged cards are major issues to be considered.
- Biometric authentication: finger prints; facial geometry; retinal and iris signatures, …
  - Distinguish real from fake
  - Type I errors reject valid image
  - Type II errors accept invalid image
  - Safety glasses and gloves
  - Social acceptability

Incident Response

- Quick risk assessment to evaluate both the effect of the attack and options to respond
- One possible response is to isolate the system
- Preparation, detection and analysis, containment, eradication, recovery
- Incident response training
- Testing of incident response capability

Symptoms

- Unusually heavy network traffic
- Out of disk space
- Unusually high CPU usage
- Creation of new user accounts
- Attempted or actual use of admin accounts
- Locked out accounts
- Account in use when the user is not at work
- Cleared log files
- Full log files with unusually large number of events
- Antivirus or IDS alerts

Symptoms

- Disabled antivirus and other security controls
- Unexpected patch changes
- Machines connecting to outside IP addresses
- Requests for information about the system (social engineering)
- Unexpected changes in configuration settings
- Unexpected system shutdown

Maintenance

- Routine
- Preventative
- Local and remote tools
- Management of maintenance personnel

Media Protection

- Safe and secure maintenance
- Guidance for transporting, handling, erasing and destroying these assets
- Safe storage from loss, fire, theft, unintentional distribution or environmental damage
- The use of unauthorized removable media should not be permitted (to prevent the introduction of malware or theft of data)
- If possible use mechanized enforcement

Physical and Environmental Protection

- Closely tied to plant safety, aiming to prevent:
- Unauthorized physical access
- Physical modification, manipulation, theft or destruction
- Unauthorized observation (visual, note taking, photographs …)
- Unauthorized introduction of new systems etc.
- Unauthorized introduction of new devices to manipulate, eavesdrop or cause other harm

Defense-in-Depth and Physical Security

- Protection of physical locations
- Access control
  - Access monitoring systems
  - Access limiting systems
- People and asset tracking
- Environmental factors – dust, vibration, temperature and humidity
- Environmental control – HVAC
- Power – uninterruptable power supply

Planning

- Security plan should cover
  - Architecture procurement
  - Installation
  - Maintenance
  - Decommissioning
- Emerging ICS security capabilities
- New threats discovered by organisations such as ICS-CERT

Personnel

- Hiring policies – background checks; interview process; expectations
- Organization policies and practices: security; information classification; document and media maintenance and handling; training; acceptable usage; performance reviews; …
- Terms and conditions of employment

- Risk Assessment; System and Services Acquisition

System and Comms Protection

- Encryption – latency, key management
- VPN – secure access from an untrusted network to the ICS network.
- Common VPN technologies:
  - IPsec – interoperability issues because of vendor specific extensions
  - SSL
  - SSH

System and Information Security

- Virus and Malicious Code Detection
- Intrusion Detection and Prevention
- Patch Management

Privacy Controls

- Authority and Purpose
- Accountability, Audit and Risk Management
- Data Quality and Integrity
- Data Minimization and Retention
- Individual Participation and Redress
- Security
- Transparency
- Use Limitation