Setting the Standard for Automation™

Using the ISA/IEC 62443 Standard to Secure Your Control Systems

Course IC32E (Online)
Participant Noteset
Volume I

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

ISA Cyber Instruction – IC32E
Online Instructor-Led Course

Using the ISA/IEC 62443 Standard to Secure Your Control Systems

This online/self-study course focuses on the issues involved in developing a cyber security program for industrial automation and control systems including risk assessment, awareness of cyber threats and exploits and the use of 'countermeasures' to reduce risk and/or mitigate the consequences of a successful cyber-attack. This course will aid engineering personnel with responsibility for plant/process automation systems in identifying potential vulnerabilities and implementing changes to improve the cyber security of their critical process automation systems.

The course is divided into twelve (12) separate modules, with a recommended one module or two module per week for completion. However, students may work at their own pace, provided they cover the material by the indicated review dates.

Various learning techniques will be provided to cover the weekly course areas including: pre-recorded instructor presentations, additional resources, homework assignments, reading assignments, as well as live Q&A debrief instructor sessions. Refer to your detailed course syllabus, which is provided with your course materials, for further information/instructions.

Course Schedule

Pre-Survey
Students will be asked to take a pre-survey, which includes questions related to the subject matter areas. Answers will be provided for students to assess their knowledge, prior to beginning the course materials.

Module 1: Introduction to Control Systems Security

Module 2: ISA/IEC 62443-1-1 Terminology and Regulations & Standard

Module 3: ISA99 Committee, The 62443 Standards, and Intro to the IACS Cybersecurity Lifecycle

Module 4: Establishing an Industrial Automation and Control Systems Security Program

Module 5: Industrial Networking Basics L1 - L7

Module 6: Demonstration Lab: PCAP Analysis Industrial Protocols

Module 7: Network Security Basics

Module 8: Industrial Protocols

Module 9: ISA/IEC 62443 Models

Module 10: Network Segmentation, Patch Management, and Intrusion Detection

Module 11: Security Risk Assessment and System Design Intro

Module 12: Security Program Requirements for IACS Service Providers

Post-Survey

Students will be asked to take a post-survey, which includes questions related to the subject matter areas. Answers will be provided for students to assess their knowledge, prior to beginning the course materials.

Final Examination

Thank you...

ISA Training Equipment Donors

ISA would like to thank the following companies for donating equipment for use in our hands-on training labs. By donating equipment, these companies have increased their name recognition within the industry while helping ISA continue its efforts to offer superior automation and control training.

ABB Instrumentation, Inc.
BELDEN SENDING ALL THE RIGHT SIGNALS
FLUKE
MARSH BELLOFRAM Group of Companies
Rockwell Automation
Allen-Bradley
CALA Engineering Services Inc.
invensys FOXBORO
metso automation
SIEMENS
ASHCROFT INSTRUMENT DIVISION DRESSER
EMERSON Process Management
frontline www.fte.com
MOORE INDUSTRIES WORLDWIDE
STEEPLECHASE SOFTWARE THE UNDISPUTED LEADER IN PC CONTROL
BadgerMeter,Inc.
Emerson Process Management- Rosemount Measurement
HART SCIENTIFIC
MOXA
TRERICE TEMPERATURE · PRESSURE · CONTROL
beamex - master of calibration -
Endress+Hauser The Power of Know How
Honeywell
PHOENIX CONTACT
Wade Associates, Inc.
JMS SOUTHEAST INCORPORATED
Prime Technologies
WEST Temperature Control Solutions

Learn more with ISA's hands-on Portable Training Labs!

Our hands-on labs are ready to ship to your facility. Offering state-of-the-art equipment and expert instruction, ISA Onsite Training brings automation training directly to you.

Learn more at www.isa.org/OnsiteTraining.

Setting the Standard for Automation™

ISA™

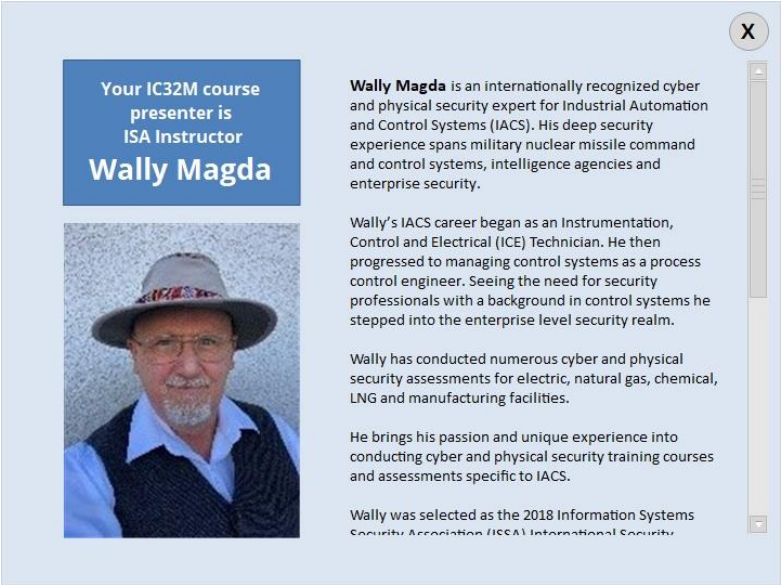
Week 1

Setting the Standard for Automation™

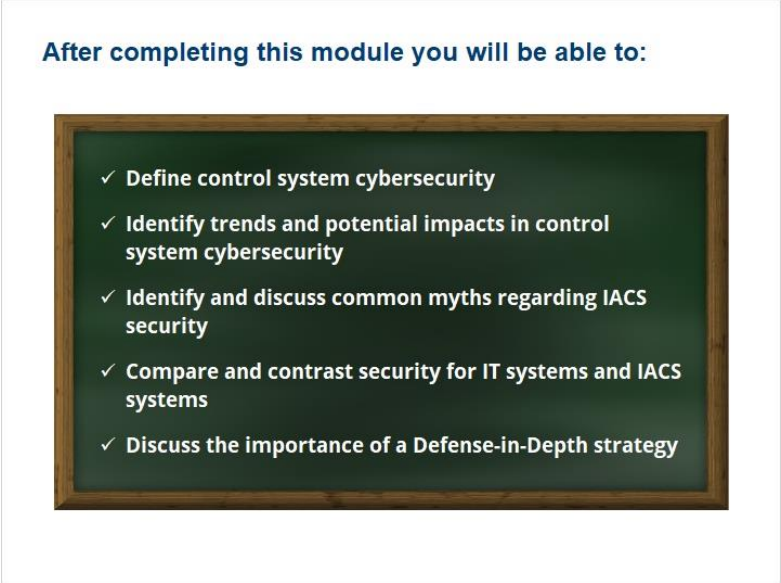
ISA IC32M Module 1

Course Contributors (Slide Layer)

Course Presenter (Slide Layer)



1.5 In this module



Notes:

After completing this module, you will be able to:

- Organize and facilitate a cybersecurity risk assessment for an IACS
- Identify and evaluate realistic threat scenarios
- Identify and assess the effectiveness of existing countermeasures
- Identify gaps in existing policies, procedures and standards

Trends in Control System Cybersecurity

- Businesses have reported more unauthorized attempts and marked increase in malicious code attacks
- Controls systems use more commercial off the shelf (COTS) software and hardware
- Implementing Internet Protocols (IP) exposes control systems to same vulnerabilities as business systems
- Increased use of remote monitoring and access
- Tools to automate attacks are commonly available

Potential Impacts

Large scale consequences could include:

- ✓ Threat to a nation's security
- ✓ Loss or damage of national electric grid
- ✓ Military capability degraded by extended electrical and fuel supply outages
- ✓ Telecommunications
- ✓ Water supply
- ✓ Hospitals

- ✓ Unauthorized access, theft or misuse of data
- ✓ Loss of integrity or reliability of the control system
- ✓ Loss of control system availability
- ✓ Equipment damage
- ✓ Personnel injury
- ✓ Violation of legal and regulatory requirements

Notes:

- Potential impacts include threat to a nation's security
- Loss or damage of national electric grid
- Military capability degraded by extended electrical and fuel supply outages
- Telecommunications
- Water supply
- Hospitals

Notes:

- Malware as a service (MaaS) and related variants are creating a market for malicious software and distributed targeting that have gained a great deal of popularity in the last four years
- Bad actors take VISA and paypal or bitcoins
- Some even have guaranteed customer satisfaction help desks and offer double-your-hack-back if not satisfied

Notes:

The Cybercrime report from Malware Byes shows a continued uptick in the detection of ransomware. Trojan variations are up by over 200%.

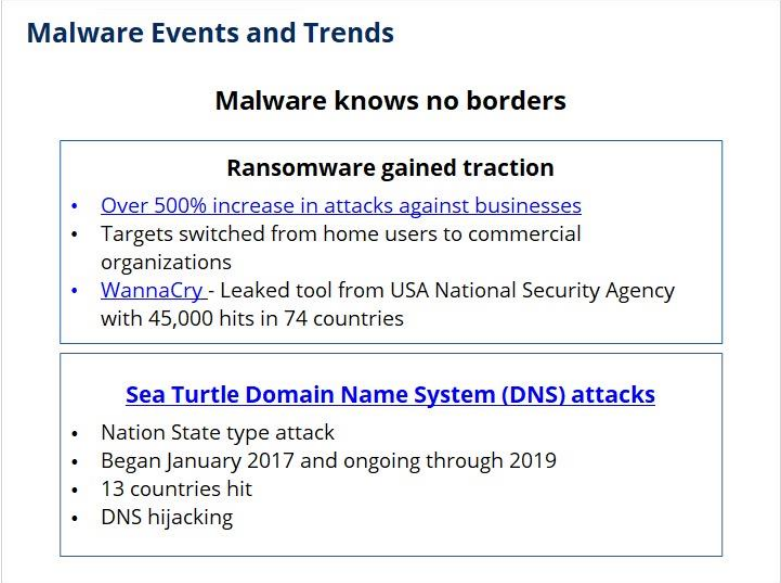
Let's look at an example of a recent ransomware attack which occurred 19 March 2019 at the global aluminum solutions company - Norsk Hydro. The financial impact in the first quarter on 2019 was estimated to be equivalent to between 46 and 52 million US dollars. There is evidence that recon was done prior to the attack. Kudos to Norsk Hydro for being fairly open about cyber attack.

This loss was small compared to $100 millions in damages Spanish food giant Mondelez and the $300 million figure reported by Danish shipping giant Maersk when hit by ransomware in 2017.

Cyber insurance coverage may not pay.

https://www.zdnet.com/article/norsk-hydro-ransomware-incident-losses-reach-40-million-after-one-week/ (retrieved 5 May 2019)

https://www.zdnet.com/article/notpetya-an-act-of-war-cyber-insurance-firm-taken-to-task-for-refusing-to-pay-out/ (retrieved 27 July 2019)



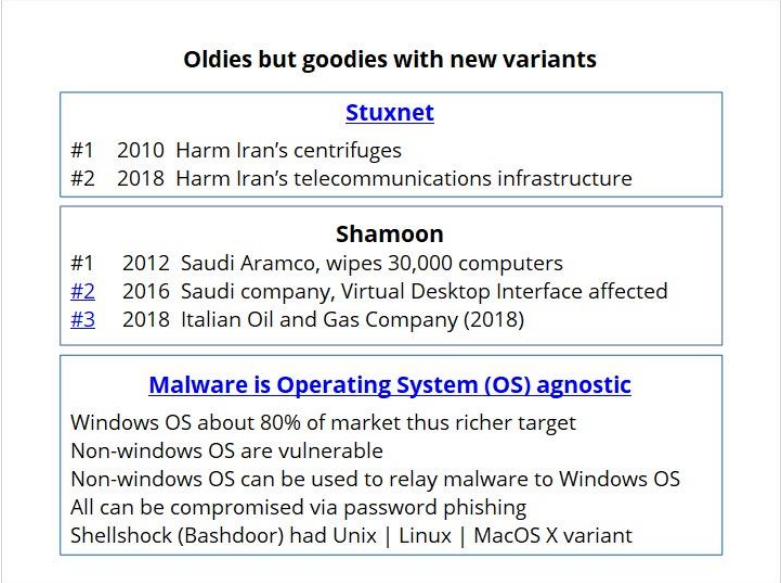
Notes:

Ransomware over 500% increase in attacks against businesses Q1 2019

- https://www.bleepingcomputer.com/news/security/over-500-percent-increase-in-ransomware-attacks-against-businesses/
- WannaCry 2017
- https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/#d9ac26ae599b

Sea Turtle Established a means to control the DNS records of the target.

- Modified DNS records to point legitimate users of the target to actor-controlled servers.
- Captured legitimate user credentials when users interacted with these actor-controlled servers.
- https://www.wired.co.uk/article/dns-hijacking-hack-seaturtle-cisco
- https://blog.talosintelligence.com/2019/04/seaturtle.html



Notes:

- Stuxnet claimed to be first global digital weapon
    - https://www.cybersecurity-insiders.com/iran-says-israel-launched-stuxnet-2-0-cyber-attack/
- Shamoon #1 erased data, bricks hard drive
    - Left image of a burning American flag
- Shamoon #2 Impacts one of the primary countermeasures employed against wiper attacks: Virtual Desktop Interface snapshots.
    - https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/ (retrieved 6 May 2019)
- Shamoon #3 Malware Variant Targets Italian Oil and Gas Company
    - https://thehackernews.com/2018/12/shamoon-malware-attack.html
- Malware OS agnostic
    - https://www.statista.com/statistics/218089/global-market-share-of-windows-7/
    - https://www.linux.com/news/2017/7/linux-malware-rise-look-recent-threats
    - Shellshock (Bashdoor) example of exploit possible on unpatched systems (2014)

Notes:

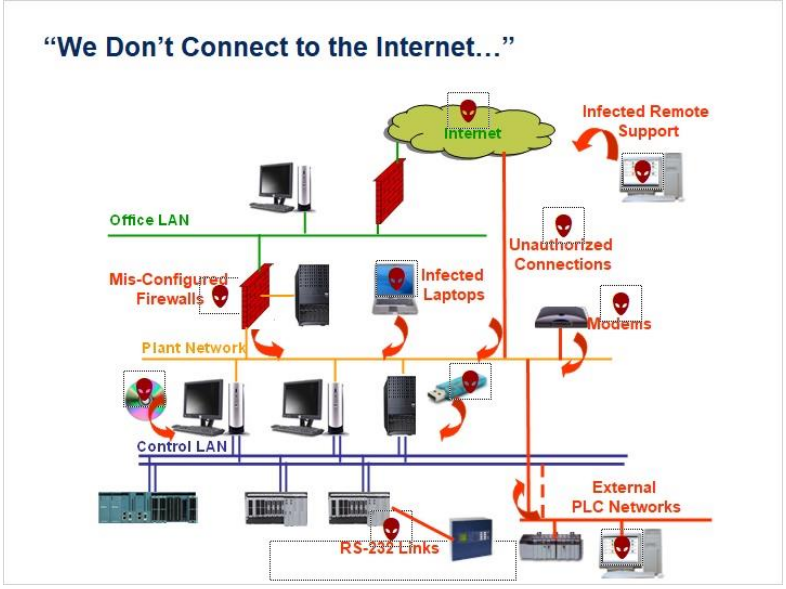
Probably the most common myth concerning the cybersecurity of an IACS is the misconception of **"We don't connect to the Internet."** An IACS may not be directly connected to the Internet, however connections to the company business network, use of USB drives or separately maintained laptops, even RS232 use of Ethernet media converters can expose an IACS to potential hackers.

In 2008, Project Shine set out to establish a baseline for the number of IACS devices were connected to the Internet. The project relied on Shodan, a search engine for Internet-connected devices. By 2014, the project had identified over one million Internet connected SCADA and IACS devices. More recent numbers indicate that organizations are

taking measures to avoid having IACS devices exposed to the Internet. The main reason these devices are Internet accessible is to save time and money. A single technician can maintain an infrastructure from anywhere in the world! It saves a lot of money and is the way of the future, you just need to pay attention to how you do it.

Real world vulnerability assessments found across the industry can typically reveal

- infected remote support
- mis-configured firewalls
- infected laptops
- unauthorized connections
- infected CDs or USB sticks
- RS-232 links and
- external PLC networks.



Notes:

- RS232 use of Ethernet media converters provide opportunity to use internet

Notes:

Myth #2 Control Systems are behind a firewall.

Myth 3 Hackers Don't Understand Control Systems

- This is no longer true
- Hacking is no longer just for fun – hackers now sell zero-day exploits to organized crime
- Hacking as a service has hit the mainstream
  - No longer only on underground dark web
  - Jobs put out to bid
- SCADA and process control systems are now common topics at "DEFCON" and "Blackhat" conferences

Notes:

- Another trend that has become more significant with time is **crime**.
- **Hacking** has moved from a hobbyist pursuit with a goal of notoriety to a criminal pursuit with a goal of money. Hackers can sell unknown vulnerabilities-'zero-day exploits'-on the black market to criminals who use them to break into computers. Hackers with networks of hacked machines or botnets can make money by selling them to spammers or phishers. They can use them to attack networks. We are seeing more and more criminal extortion over the Internet: hackers with networks of hacked machines threatening to launch DoS attacks against companies.
- These attacks started against fringe industries- online gambling, online computer gaming, online pornography-and against offshore networks. They are now attacking mainstream businesses and becoming more commonplace
- From NISCC Report on Targeted Trojan Attacks: "Trojan capabilities suggest that the covert gathering and transmitting of otherwise privileged information is a principal goal. The attacks normally focus on individuals who have jobs working with commercially or economically sensitive data."

1.19 Myth #3

Notes:

- Hopefully issues are corrected prior to disclosure
- Advisories and Alerts updating daily
- https://ics-cert.us-cert.gov/advisories (retrieved 3 July 2017)
- https://ics-cert.us-cert.gov/alerts (retrieved 3 July 2017)

Notes:

Is your IACS a target? Don't be so sure.

Notes:

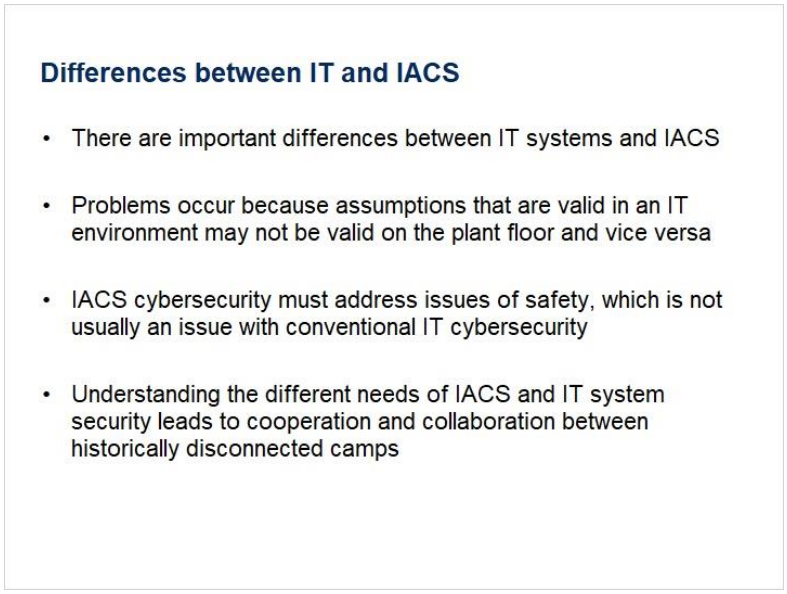
- Here are 290 companies in 2016 that may have thought they were not a target
- Slides from US ICS-CERT Year in review report
- USA statistics. However ICS-CERT does deploy upon request of other nations
- 2017 report has similar numbers. ICS-CERT did not provide 2017 pie chart
- Received roughly 106,000 incident reports from Federal, state, local, tribal, territorial governments, private sector, affecting communications and control systems.
- No information provided yet for 2018
- https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_IR_Pie_Chart_S508C.pdf (retrieved 6 may 2016)
- https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_Year_in_Review_2017_Final.pdf (retrieved 6 may 2016)

Notes:

- Here are 290 companies in 2016 that may have thought they were not a target
- Slides from US ICS-CERT Year in review report
- USA statistics. However ICS-CERT does deploy upon request of other nations
- 2017 report has similar numbers. ICS-CERT did not provide 2017 pie chart
- Received roughly 106,000 incident reports from Federal, state, local, tribal, territorial governments, private sector, affecting communications and control systems.
- No information provided yet for 2018
- https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_IR_Pie_Chart_S508C.pdf (retrieved 6 may 2016)
- https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_Year_in_Review_2017_Final.pdf (retrieved 6 may 2016)

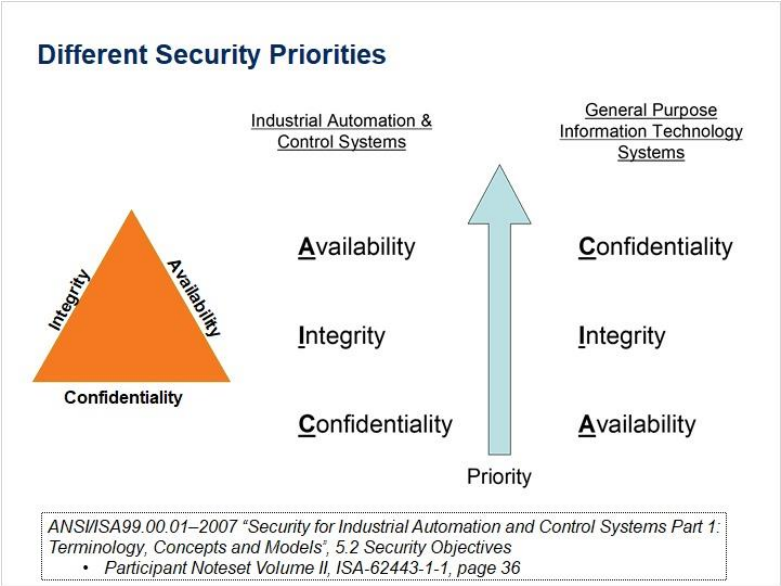
Notes:

- Layers of Protection Analysis (LOPA)
- Point out the Safety system automatic shutdown
- internet attack could defeat even the most sophisticated Safety Integrated System/Safety Integrity Level (SIS/SIL)



Notes:

- Part 1-1, Introduction, page 14 states: Because mutual understanding and cooperation between information technology (IT) and operations, engineering, and manufacturing organizations is important for the overall success of any security initiative, this standard is also a reference for those responsible for the integration of industrial automation and control systems and enterprise networks.



Notes:

- Information security typically includes three properties, confidentiality, integrity, and availability, which are often abbreviated by the acronym "CIA" and depicted as a triangle
- An information technology security strategy for typical "back office" or administrative systems may place the primary focus on confidentiality and the necessary access controls needed to achieve it.
- Integrity might fall to the second priority, with availability as the lowest.
- In the industrial automation and control systems environment, there is generally an inversion of these properties with availability and integrity more important to IACS.
- Protecting proprietary batch processes and recipes may take a higher precedence
- Security in these systems is primarily concerned with maintaining the availability of all system components.
- There are inherent risks associated with industrial machinery that is controlled, monitored, or otherwise affected by industrial automation and control systems
- Usually confidentiality is of lesser importance, because often the data is raw in form and must be analyzed within context to have any value.

Different Performance Requirements

IT	IACS
Response must be reliable	Response **is time critical**
High throughput	Modest throughput
High delay and jitter tolerated	High delay is a serious concern
Less critical emergency interaction	Response to emergencies is critical
IT protocols	IT and industrial protocols

Notes:

A typical sample of differences is presented here over the next 4 slides to elicit thought and discussion
IACS has a lot to learn regarding network design, hardware selection, etc. and pointing this out as a difference would be helpful.
IT generally understands the separation concept but thinks IACS can stick business level switches and network design at the IACS layer.

Different Availability Requirements

IT	IACS
Scheduled operation	Continuous operation
Occasional failures tolerated	Outages intolerable
Rebooting tolerated	Rebooting may not be acceptable
Beta testing in the field acceptable	Thorough QA testing expected in non-production environment
Modifications possible with little paperwork	Formal certification may be required after any change

- Need to understand the reliability impacts of information security technologies before deploying.
- Example: Installing a service pack in the pharmaceutical industry requires an expensive recertification of the system.

Different Operating Environments

IT	IACS
Typical “Office” Applications	Special Applications
Standard OS’s	Standard and embedded OS’s
Upgrades are straightforward	Upgrades are challenging and may impact hardware, logics and graphics
Technology is refreshed often Commercial Off The Shelf (COTS) (3 to 5 years)	Legacy systems (15-20 years)
Abundant resources (memory, bandwidth)	Resource constrained
Data center, server room or office environment	Industrial environment

Notes:

- COTS has become more common in IACS over the last few years

Different Risk Management Goals

IT	IACS
Data confidentiality and integrity are paramount	HSE and production are paramount (integrity & availability)
Risk impact is loss of data, delay of business operations	Risk Impact is loss of life, equipment or product
Recover by reboot	Fault tolerance essential

Example: **Password lockout procedures**:

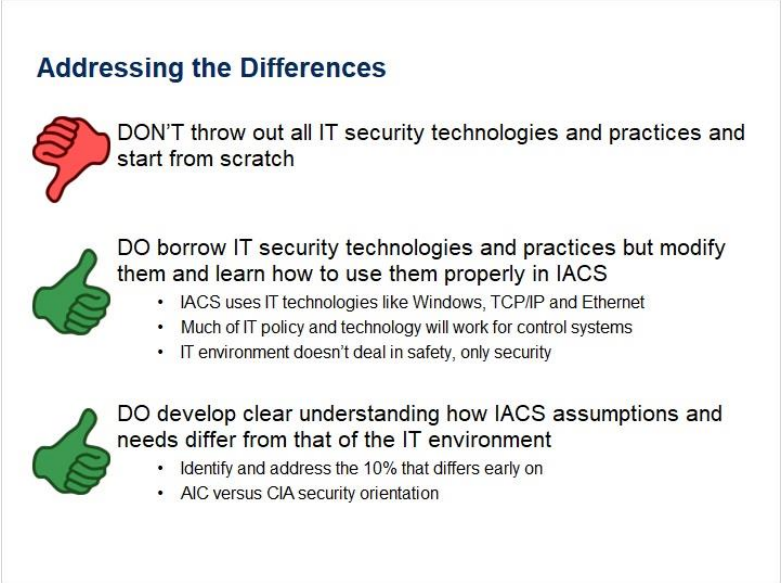
- IT: Lockout ALL access for the 10 minutes after 3 failed login attempts.
- IACS: Make operator access easy and foolproof.

Operator panics during chlorine leak and miss-spells his password three times. HMI lockouts ALL access for 10 minutes.

- The outcome can be disastrous

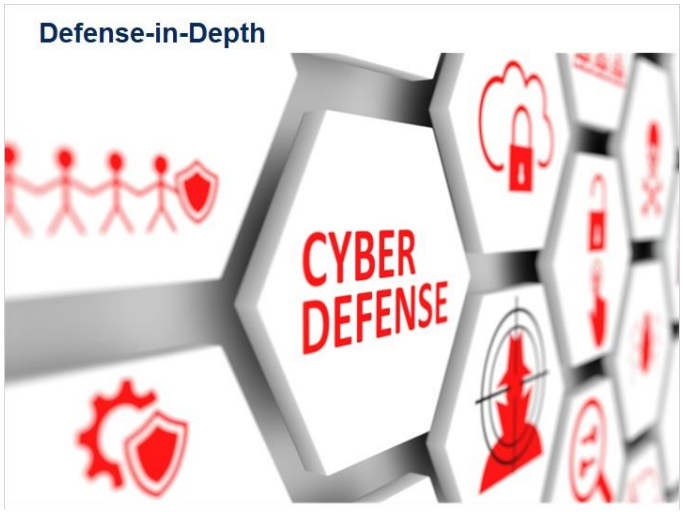
Notes:

- HSE= Health Safety & Environment



Notes:

- Good reference article on ISA site
- https://automation.isa.org/top-10-differences-ics-cybersecurity/ (retrieved 7 May 2019)
- Authors use term ICS versus IACS, for our purposes we will consider the terms one and the same



Defense-in-Depth

A Perimeter Defense is Not Enough

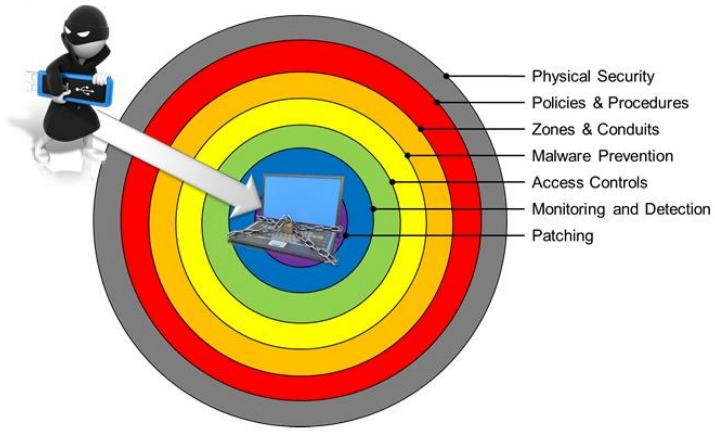
- ⇨ The bad guys will eventually get in
- ⇨ Can't just install a firewall and forget about security
- ⇨ Must harden the control systems network

You need:

- ✓ Defense in Depth
- ✓ Detection in Depth
- ✓ Accountable and timely incident response

Defense-in-Depth

"Defense in Depth" – applying multiple countermeasures in a layered or stepwise manner.



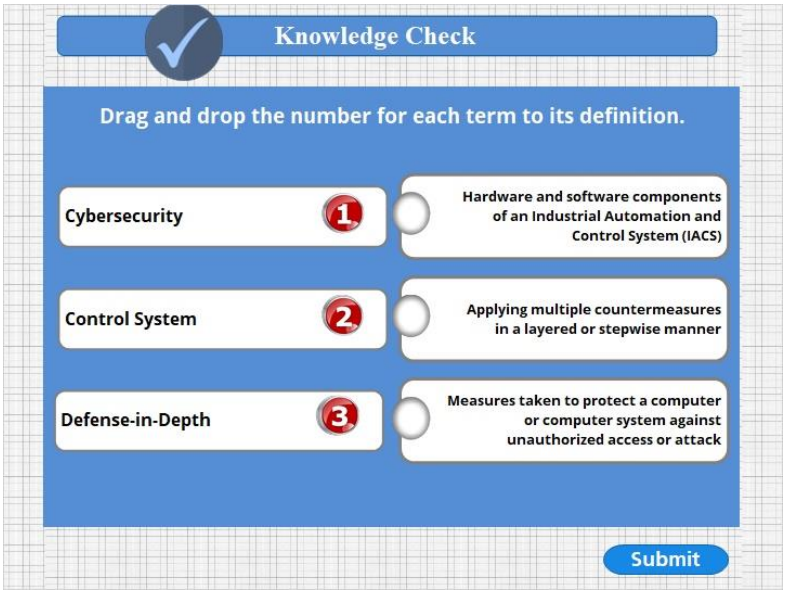
Detection in Depth

There should be alarms, logs, and detection methods to identify:

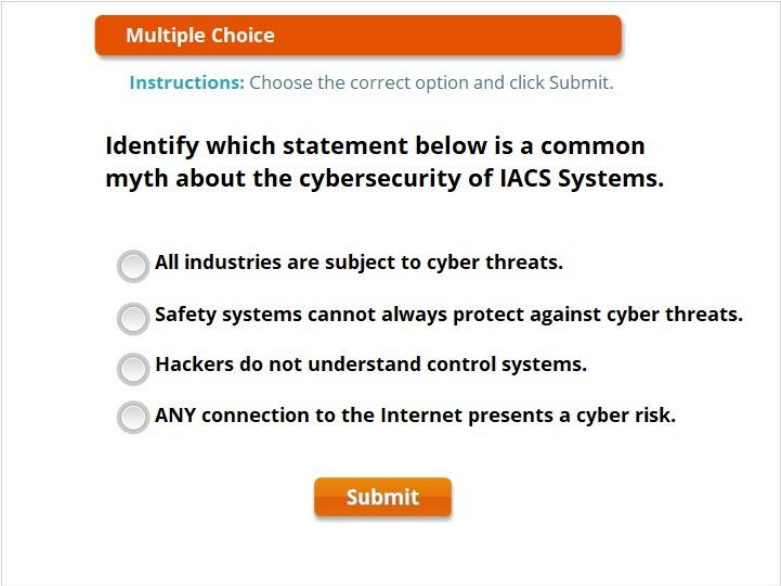
- Unusual data transfer patterns
- Unexpected protocols being used
- Out-of-time data traffic
- Communication to unknown or unexpected MAC or IP Addresses
- Logs should be turned-on to monitor activity
  - Send SYSLOG compatible logs to a central logging server
- Firewalls and IDS should be configured to identify any traffic that is not part of the expected traffic across zones
- Patch Management & Anti-virus should report devices out-of-date
- Detection of unknown devices
- Detection of missing devices

Notes:

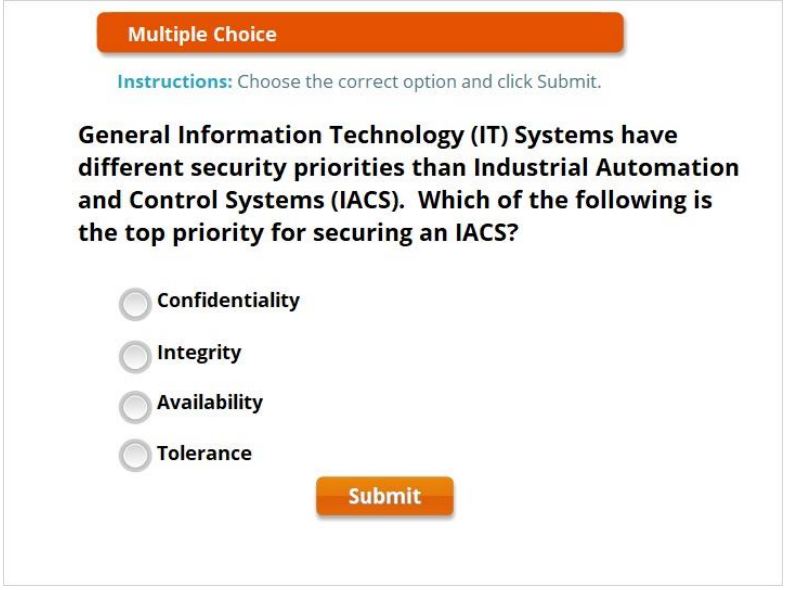
- a) **Design the risk out - One form of mitigation is to change the design of the system so the risk is** removed.
- Some risks exist simply because access is available to something to which no access ever needed.
- Completely disabling the unnecessary function or "welding" the function from access can mitigate the risk.
- Organizations can make the appropriate business decisions so the risk is not taken.
- This response may involve saying no to something, whether a new vendor product, system, or relationship.
- b) **Reduce the risk - Risks can be decreased to an acceptable level through the implementation of** countermeasures that reduce the likelihood or consequence of an attack.
- The key here is to achieve a level of "good enough" security, not to eliminate the risk.
- c) **Accept the risk - There is always an option to accept the risk, to see it as the cost of doing business**.
- Organizations must take some risks, and they cannot always be cost effectively mitigated or transferred.
- d) **Transfer or share the risk - It may be possible to establish some sort of insurance or** agreement that transfers some or all of the risk to a third entity.
- A typical example of this is outsourcing of specific functions or services.
- This approach cannot always be effective, because it may not always cover all assets completely.
- An electronic security policy can recover certain damages, but not logical assets such as loss of customer confidence.
- e) **Eliminate or redesign redundant or ineffective controls -**
- A good risk assessment process will identify these types of controls that need to be addressed so that more attention can be focused on controls that are effective and efficient.
- ISA99 Committee Work Products - July 2014



Drag Item
2
3
1

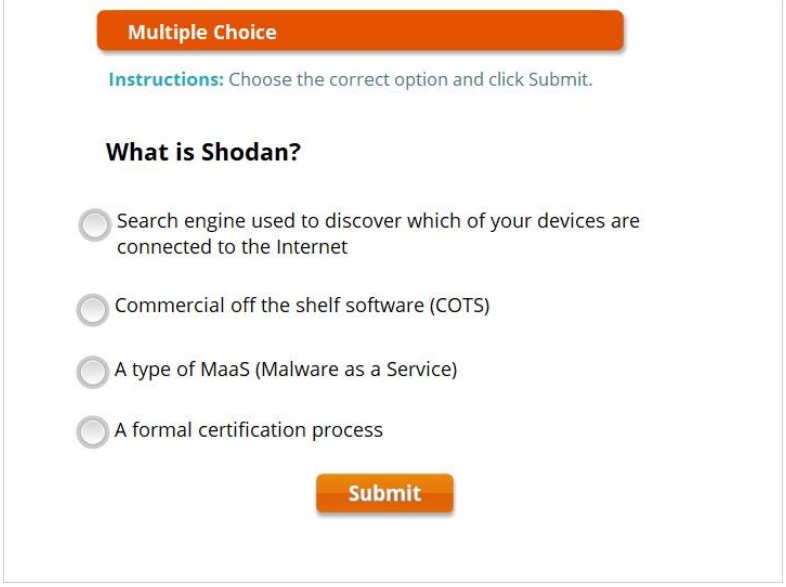


Correct	Choice
	Radio Button 1
	Radio Button 2
X	Radio Button 3
	Radio Button 4

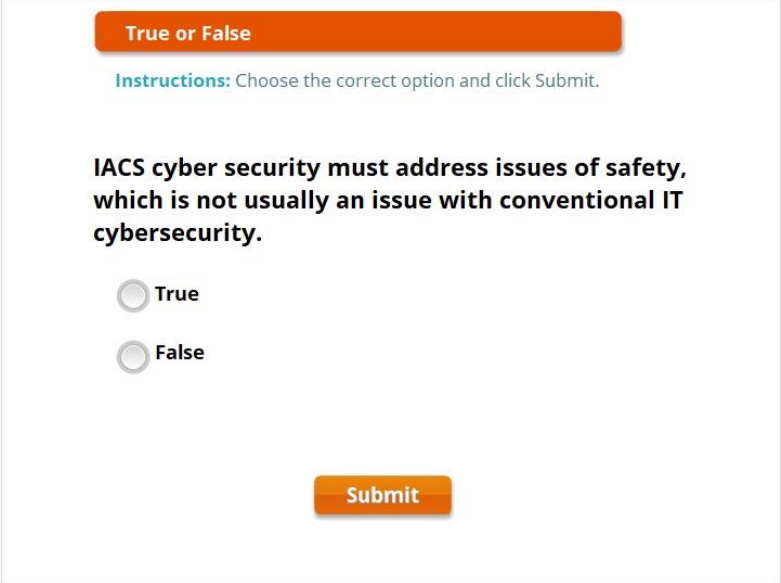


Correct	Choice
	Radio Button 1
	Radio Button 2
X	Radio Button 3
	Radio Button 4

Correct	Choice
	Radio Button 1
X	Radio Button 2



Correct	Choice
X	Radio Button 1



Correct	Choice
X	Radio Button 1
	Radio Button 2

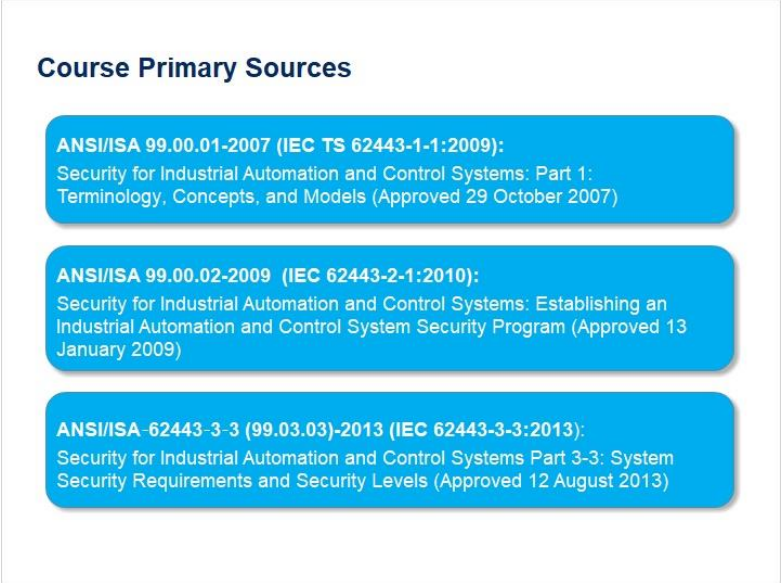
Week 2

ISA IC329 Module 2

After completing this module you will be able to:

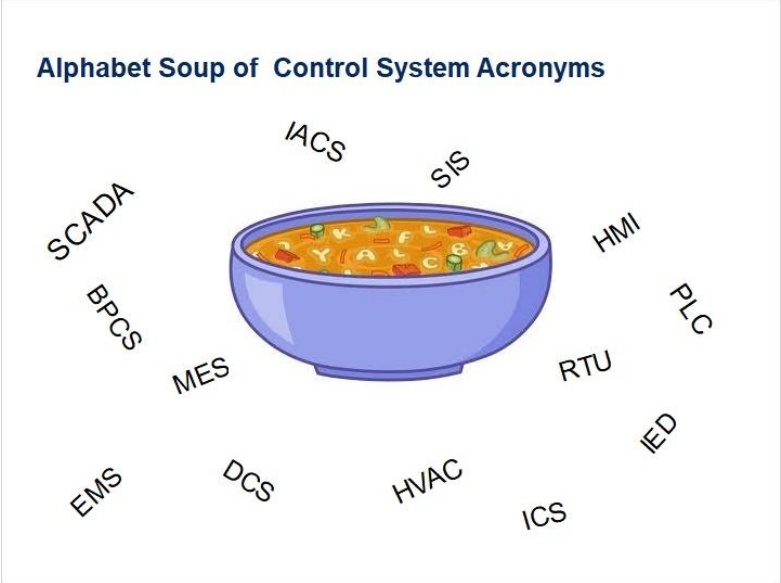
- ✓ Identify ISA/IEC 62443 as the focus of this course.
- ✓ Differentiate between IACS and ICA.
- ✓ Recognize regulations in the industry may be mandatory and may include limitations.
- ✓ Recognize compliance with standards is voluntary.
- ✓ Explain the difference between normative and informative elements.
- ✓ Discuss the use of global frameworks to provide a common taxonomy and mechanism for organizations.
- ✓ Develop an awareness for the SDOs in your industry.

ISA/IEC 62443 Series Overview



Notes:

- ANSI / ISA 99.00.01-2007 **(IEC TS 62443-1-1:2009)**
  - **Technical Specification (TS)** is just a level below IEC International Standard
  - **TS** issued when global consensus to make it a standard is not reached within a designated time
- ANSI / ISA 99.00.02-2009 **(IEC 62443-2-1:2010)** is an IEC International Standard
- ANSI/ISA-62443-3-3 (99.03.03)-2013 **(IEC 62443-3-3:2013)** is an IEC International standard
- 1-1 & 2-1
- We will refer to other ISA standards/technical reports in this course but these three are the primary sources.



Notes:

- History and variety of systems used in Industrial Control led to many terms and acronyms
- Point made here is that there are lots of acronyms for similar systems and devices
- For example--One can use a PLC for controlling a portion of a refinery
    - However an organization would probably choose a DCS from a reputable vendor to control the complete facility
- Regulatory requirements such as pharma or electric grid drive use of various systems for accurate logging, alarming and control and these come with their own set of acronyms
- This course will pare down the many acronyms by focusing first on ICS and then IACS
- List of Acronyms found in Additional Resources tab and ISA99 Wiki homepage
- Just in case anyone asks here are the acronyms spelled out-there is no intent for instructor to read each acronym:
- BPCS Basic Process Control System •IED Intelligent Electronic Device
- DCS Distributed Control System •MES Manufacturing Execution System
- EMS Energy Management System •PLC Programmable Logic Controller
- HMI Human-Machine Interface •RTU Remote Terminal Unit
- HVAC Heating, Ventilation, and air-conditioning •SCADA Supervisory Control and Data Acquisition
- IACS Industrial Automation and Control System(s) •SIS Safety Instrumented System
- ICS Industrial Control System(s)

ICS or IACS?

ICS = Industrial Control System(s)

General term for types of control systems acting together to achieve an industrial objective

IACS = Industrial Automation and Control System(s)

Collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation

IACS used in ISA 62443 publications

Notes:

- History of Industrial Control development **globally** led to use of many terms and acronyms
- ICS referenced in frameworks like NIST
- There may be references to "ICS" in the IC33/34/37 courses
- For all practical purposes ICS = IACS as this course was developed
- This course will attempt to use IACS as defined by the ISA99 Committee

Terminology

- 62443 series is a large collection of related standards and reports
  - Clause 3 of each publication is go to source:

3 Terms, definitions, abbreviated terms, acronyms, and conventions .....
3.1 Terms and definitions .....
3.2 Abbreviated terms and acronyms .....
3.3 Conventions .....

- Master Glossary in development ISA-TR62443-1-2
  - Critical that there be terminology consistency across the various documents

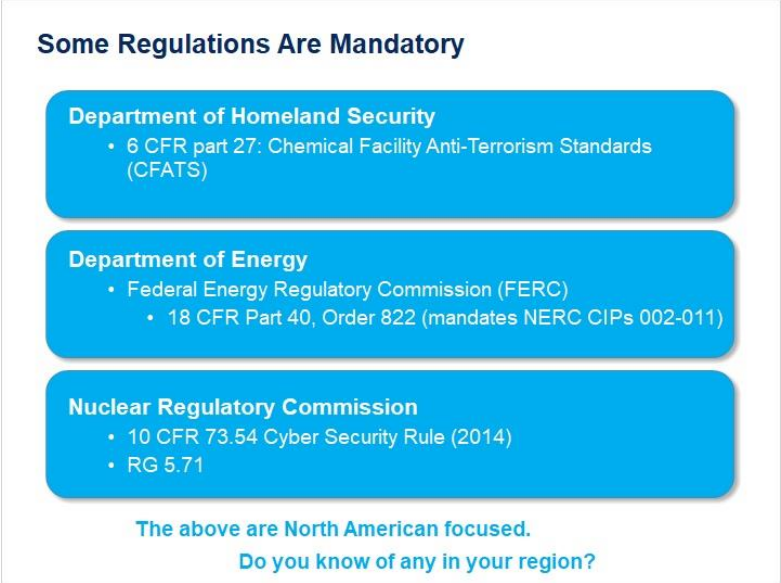
Notes:

- In the case of a large collection of related standards and reports such as those that form the ISA99 work plan it is critical that there be consistency across the various documents with respect to terminology and the concepts or elements that form the basis for the positions taken in the standards.
- With regard to terminology the committee maintains a common set of terminology for use across all committee work products

Regulations and Standards

Notes:

- Regulations are a month long course in itself; just touch on highlights in next couple of slides
- A review of publicly available information generally shows that there is a mixed resistance to mandated government frameworks and policies
- While some directives like the EC 2008/114/EC have been accepted full implementation has been slow
- http://cybersecurity.bsa.org/countries.html (retrieved 22 November 2016)
- http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf (retrieved 21 November 2016)
- http://cybersecurity.bsa.org/2015/apac/ (retrieved 22 November 2016)
- http://www.nesauae.org/nesa-compliance/ (retrieved 222 November 2016)
- NIS Directive is an EU directive regarding Cyber Security for EU countries. More info: https://www.enisa.europa.eu/topics/nis-directive



Notes:

- USA examples

Limitations

- Limited number enforced cyber and physical security regulations—no teeth
- National cyber security strategies may or may not be in place
- Public-private partnerships lacking
- Sector-specific cybersecurity plans may or may not exist
- General agreement that no country or government can address cybersecurity risk in isolation

Notes:

- A review of publicly available information generally shows that there is a mixed resistance to mandated government frameworks and policies
- Not all frameworks and regulations that do exist align well with each other even within a country
- While some directives like the EC 2008/114/EC have been accepted full implementation has been slow
- http://cybersecurity.bsa.org/countries.html (retrieved 22 November 2016)
- http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf (retrieved 21 November 2016)
- http://cybersecurity.bsa.org/2015/apac/ (retrieved 22 November 2016)
- http://www.nesauae.org/nesa-compliance/ (retrieved 222 November 2016)

Notes:

- On a bright note a number of voluntary global initiatives are in the works.
- Not all frameworks and regulations align well with each other
- ENISA list of issues commonly seen:
    - Lack of clearly identified Critical Infrastructure assets and their dependencies
    - The willingness to share information
    - Lack of personnel with IACS SCADA security skills
- While some directives like the European Commission 2008/114/EC have been accepted full implementation has been slow
- http://www.securityweek.com/agency-calls-improved-ics-security-Europe (retrieved 21 November 2016)
- https://www.enisa.europa.eu/publications/maturity-levels (retrieved 22 November 2016)
- https://cybersecuritystrategy.dpmc.gov.au/assets/pdfs/dpmc-cyber-strategy.pdf?q=270716 (retrieved 22 November 2016)
- http://cip-asia.com/japan-to-create-cyber-defense-government-agency-to-protect-scada-infrastructures/ (retrieved 22 November 2016)

Standards

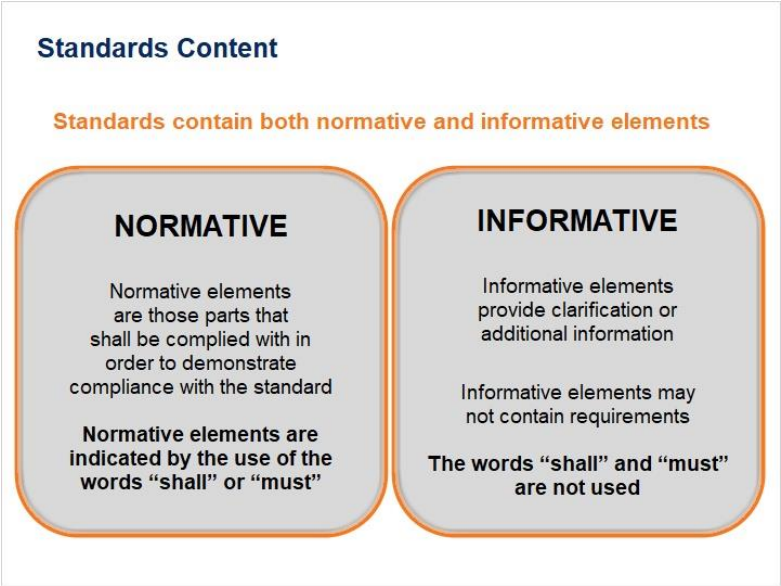
Compliance and conformance is voluntary
- Consensus driven
- Collaborative approach preferred

There is no requirement on anyone to use them unless…..
- If agreed to in a contract or referred to in regulation
- Penalty, either civil or criminal, for not complying with them

Courts may decide in the absence of relevant regulation
- Non-compliance with a standard
- Using a "what would a reasonable man on the street do" test
- Sufficient grounds to determine liability
  - EUROPEAN COMMISSION Standards and Standardization Handbook

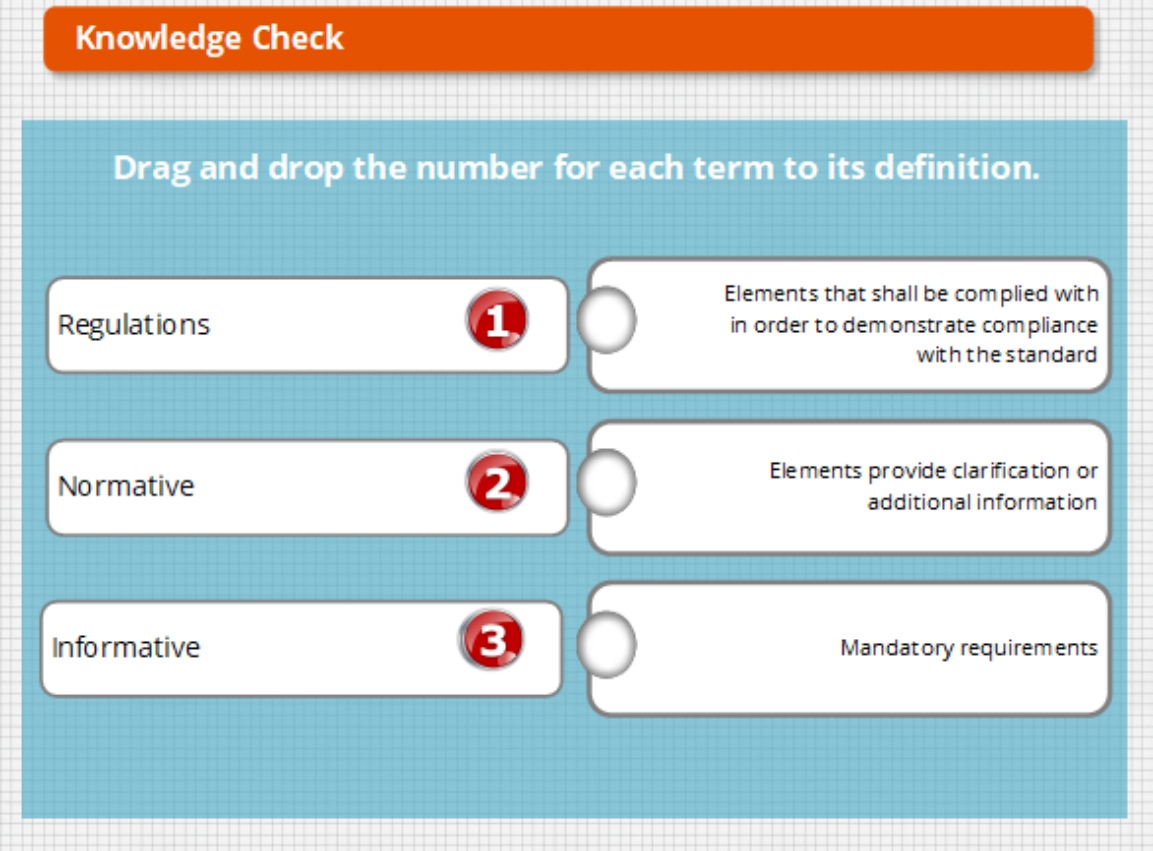
Notes:

- Intro on standards
- Man On the Street Test aka (MOST)
- Information taken from EUROPEAN COMMISSION Standards and Standardization Handbook
- http://www.iec.ch/about/globalreach/academia/pdf/academia_governments/handbook-standardisation_en.pdf (retrieved 13 Dec 2016)

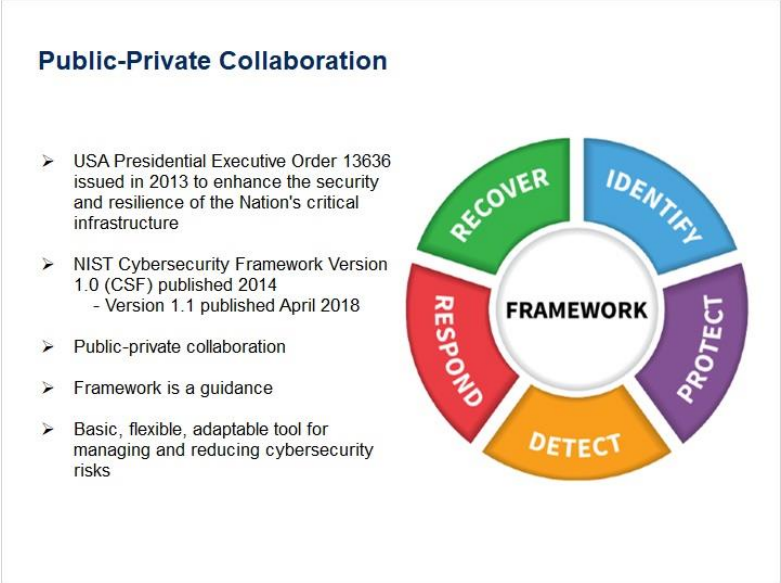


Notes:

- Discussion on "normative" and "informative" concept
- Information taken from EUROPEAN COMMISSION Standards and Standardization Handbook
- http://www.iec.ch/about/globalreach/academia/pdf/academia_governments/handbook-standardisation_en.pdf

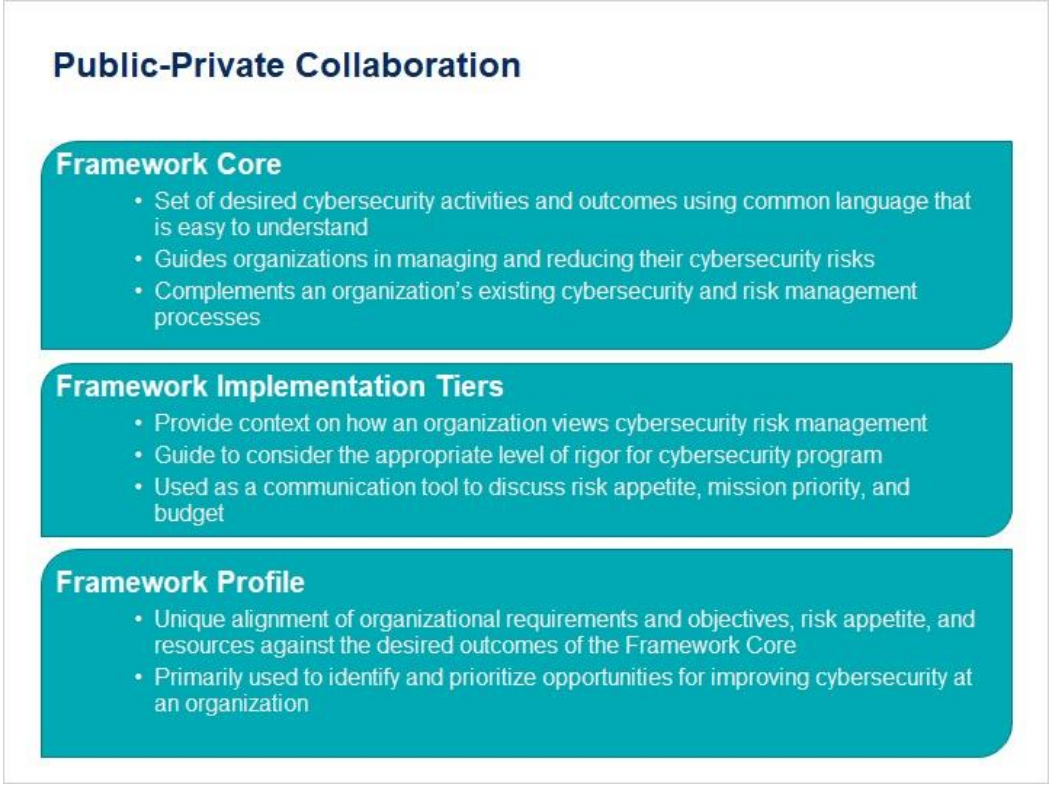


1	Oval 3
2	Oval 1
3	Oval 2



Notes:

- One of many frameworks available using “informative references” like 62443
- Typical approach for creating effective long term program security
- Maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties
- More than 3,000 people from diverse parts of industry, academia, and government participated in workshops and webinars over the 12 month period
- NIST website has a number of tools and case studies available with the CSF
- https://www.nist.gov/cyberframework (retrieved 13 May 2019)



Notes:

Designed to complement an organization's existing cybersecurity and risk management processes

Or establish a first time program

Good tool for small business that does not have a lot of IT/OT cyber resources

Graphical Representation of NIST CSF Framework

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Notes:

- Function and category Unique identifiers
- Pick a row or two and mention what is stated
- There is no intention to dig into the CSF.
- This is just one example of evolving security standards and practices

Monitor and Evaluate Applicable Legislation

Okay! So what does this "framework" have to do with using the ISA/IEC 62443 Standards to Secure Your Control Systems?

Global Frameworks

Multi-lingual Framework

CIS SAPIENZA

2015 Italian Cyber Security Report

Un Framework Nazionale per la Cyber Security

Research Center of Cyber Intelligence and Information Security
Sapienza Università di Roma

Laboratorio Nazionale CINI di Cyber Security
Consorzio Interuniversitario Nazionale per l'Informatica

Versione 1.0
Febbraio 2016

重要インフラのサイバーセキュリティを
向上させるためのフレームワーク

1.0版

米国国立標準技術研究所 (National Institute of Standards and Technology)

2014年2月12日

GUIA DE APERFEIÇOAMENTO DA SEGURANÇA CIBERNÉTICA PARA INFRAESTRUTURA CRÍTICA

Versão 1.1

إطار عمل لتحسين الأمن السبراني للبنية التحتية الحساسة

النسخة 1.1

المعهد الوطني للمعايير والتكنولوجيا (NIST)

16 أبريل، 2018

Marco para la mejora de la seguridad cibernética en infraestructuras críticas

Versión 1.1

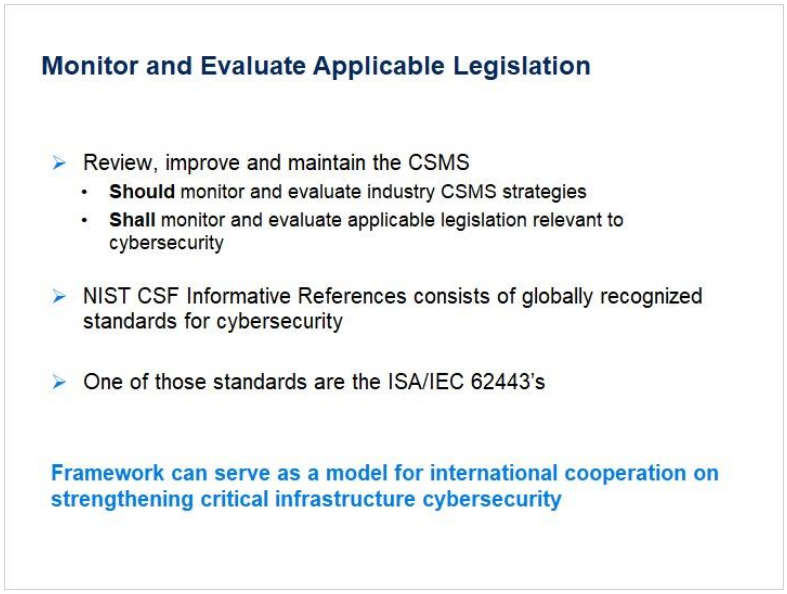
Instituto Nacional de Estándares y Tecnología

16 de abril de 2018

Notes:

Starting at top left and going clockwise:

- Italian (v1.0, not status on update)
- Japanese (v1.1 update in progress)
- Portuguese
- Spanish
- Arabic



Notes:

The 62443 standards think it is a good idea to monitor and evaluate other standards

ISA-62443-2-1 Subclause 4.4.3.6, pg 46

Monitor and evaluate industry CSMS strategies

ISA-62443-2-1 Subclause 4.4.3.7, pg 46

Monitor and evaluate applicable legislation relevant to cyber security

ISA-62443-2-1, A.4.3.6.1, f), Supporting Practices, Baseline practices, pg 153

Identifying applicable and changing regulations and legislation ….. and contractual cyber security obligations and requirements

While framework was born through U.S. policy, it is not a "U.S. only" Framework

There are a number of language translations, Arabic, Portugese, Japanese, Spanish

Monitor and Evaluate Applicable Legislation

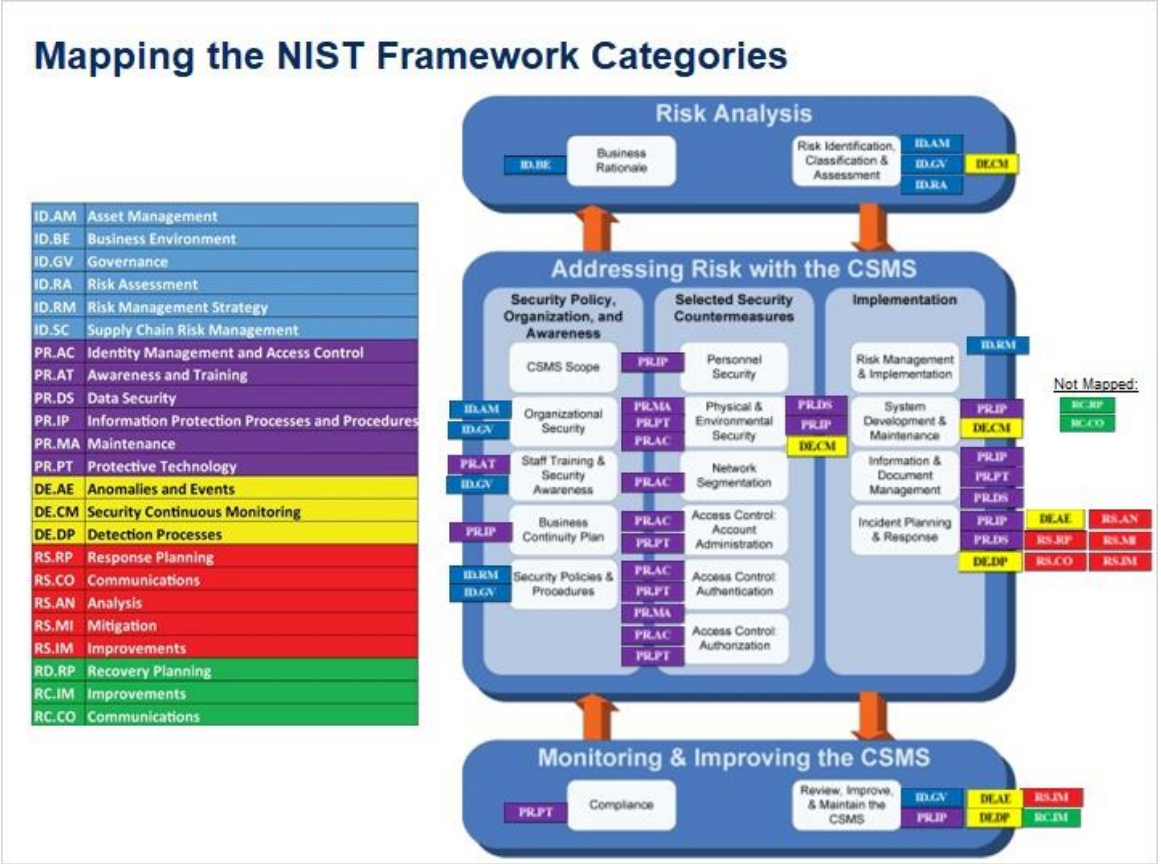
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	- **CIS CSC** 1, 5, 15, 16 - **COBIT 5** DSS05.04, DSS06.03 - **ISA 62443-2-1:2009** 4.3.3.5.1 - **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 - **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 - **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Physical access to assets is managed and protected	- **COBIT 5** DSS01.04, DSS05.05 - **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 - **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 - **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: Remote access is managed	- **CIS CSC** 12 - **COBIT 5** APO13.01, DSS01.04, DSS05.03 - **ISA 62443-2-1:2009** 4.3.3.6.6 - **ISA 62443-3-3:2013** SR 1.13, SR 2.6 - **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 - **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	- **CIS CSC** 3, 5, 12, 14, 15, 16, 18 - **COBIT 5** DSS05.04 - **ISA 62443-2-1:2009** 4.3.3.7.3 - **ISA 62443-3-3:2013** SR 2.1 - **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 - **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	- **CIS CSC** 9, 14, 15, 18 - **COBIT 5** DSS01.05, DSS05.02 - **ISA 62443-2-1:2009** 4.3.3.4 - **ISA 62443-3-3:2013** SR 3.1, SR 3.8 - **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 - **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7

Source:
National Institute of Standards and Technology (NIST)
Framework for Improving Critical Infrastructure Cybersecurity
Version 1.1 National Institute of Standards and Technology, April 16, 2018

Notes:

Excerpt to show various Informative References section with 62443 mapping

ISA 62443 highlighted in yellow



Notes:

Identify

Protect

Detect

Respond

Recover

ISA 99 named it NIST CF

62443-2-1 Edit has mapping to NIST CF and ISO

ID.SC Supply Chain Risk Management added in v1.1

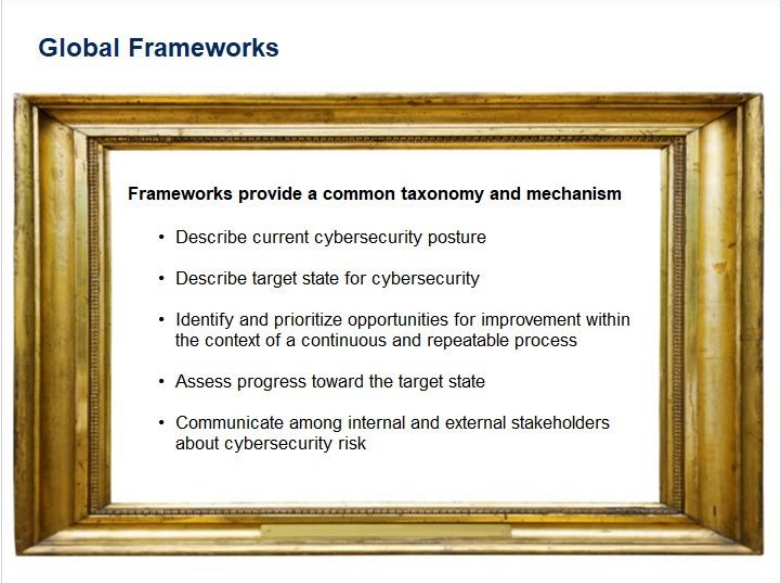
There are mappings in 62443 that could be used

Not shown on graphic:

Recovery planning RC.RP can now be mapped to 62443-2-4, SP.12.09, pg 92

Expect to see updated 62443 mapped in the next version of NIST CF

In the meantime you can map it yourself



Notes:

- Building from informative reference standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations
- In other words:
    - Here is where we are
    - Here is where we want to be
    - Here is how to get there
    - Now what can we afford?
    - Rinse, lather and repeat
- You can't fix everything
- There is no such thing as "100% security"

Notes:

Informative References used in CSF identified standards and guidelines:

ISO 27001:2013

http://www.iso.org/iso/catalogue_detail?csnumber=54534 (retrieved 13 May 2019)

ISA 62443-2-1:2009

ISA 62443-3-3-2013

COBIT 5 (Control Objectives for Information and Related Technology-ISACA)

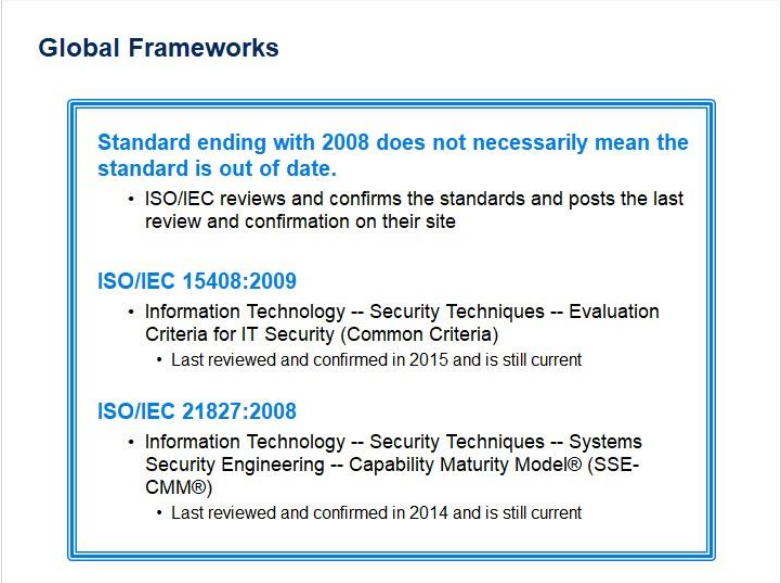
http://www.isaca.org/cobit/pages/default.aspx (retrieved 13 May 2019)

CCS CSC (Council on CyberSecurity Top 20 Critical Security Controls)

https://www.cisecurity.org/critical-controls/ (retrieved 13 May 2019)

NIST Special Publication 800-82 Rev 2

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf (Retrieved 13 May 2019)



Notes:

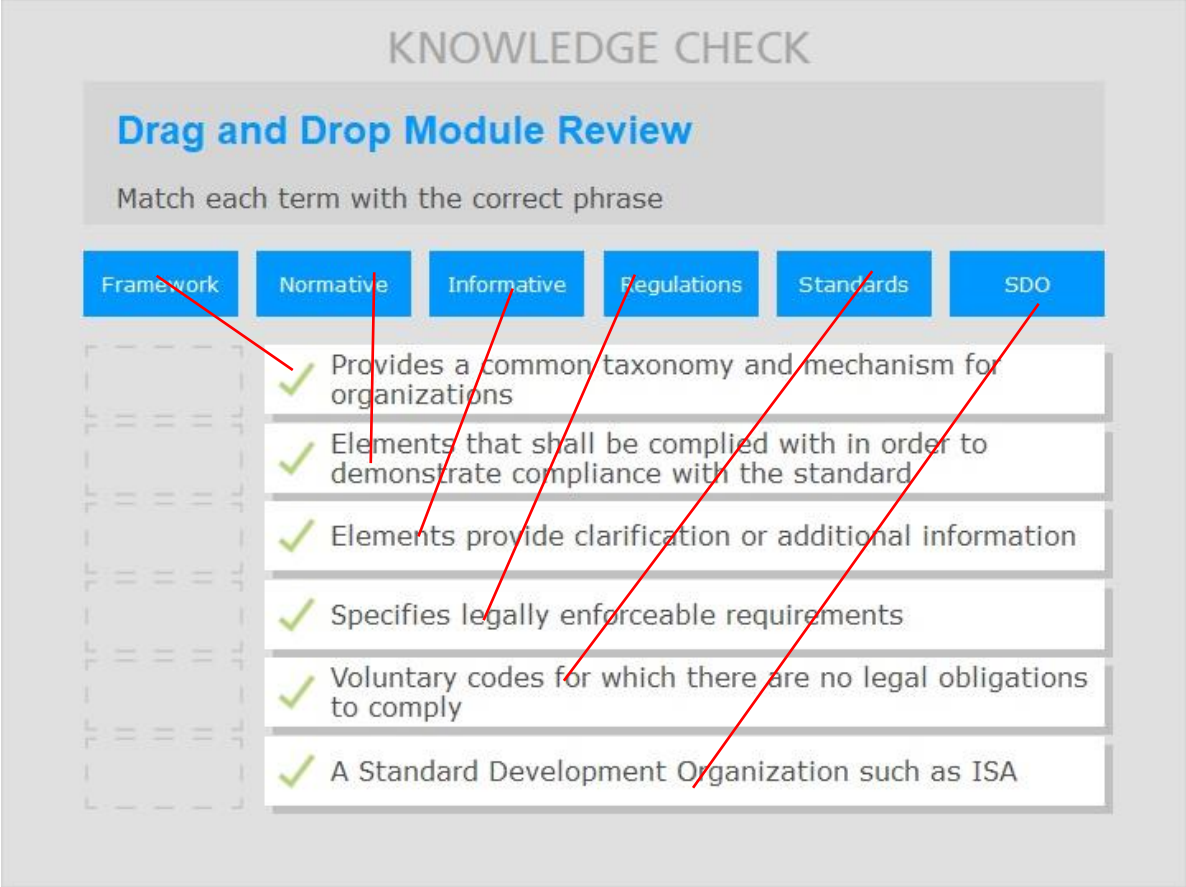
- Don't assume if the year 2008 or 2009 is in title that the standard is obsolete.
- Check source for validity and last refresh
- Examples
    - http://www.iso.org/iso/catalogue_detail.htm?csnumber=50341 (retrieved 13 May 2019)
    - http://www.iso.org/iso/catalogue_detail.htm?csnumber=44716 (retrieved 13 may 2019)

Notes:

- In your quest to review, improve and maintain the CSMS it helps to be familiar with SDO's
- SDO's have a lot of industry guidance resources.
    - May require membership
    - Your company may already be a member or sponsor

Notes:

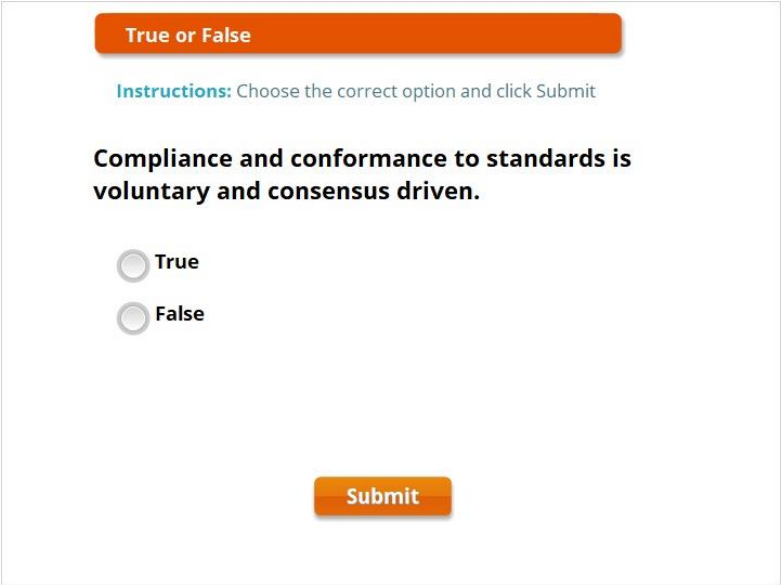
A few more notable organizations providing industry guidance and involved with SDO in one way or another



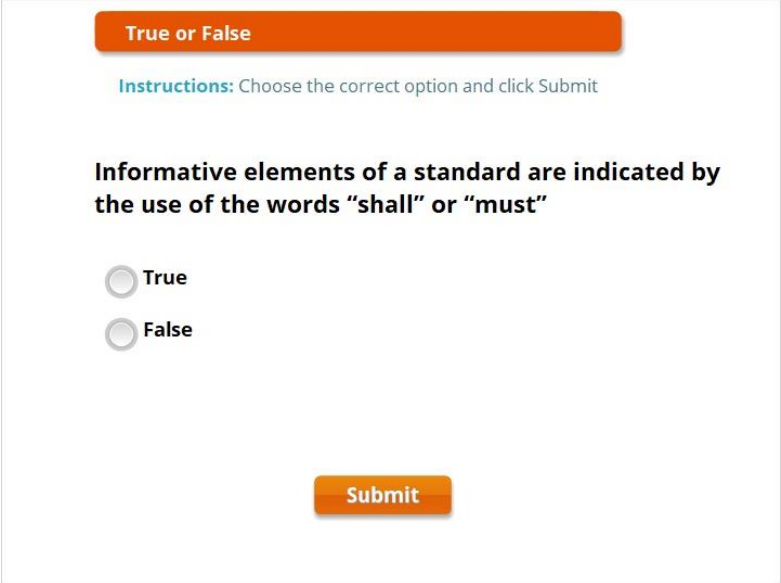
Drag Item	Drop Target
Framework	Dropzone 1
Normative	Dropzone 2
Informative	Dropzone 3
Regulations	Dropzone 4
Standards	Dropzone 5
SDO	Dropzone 6

NOTE: Answers are shuffled in the actual program so they may appear in a different order in the module.

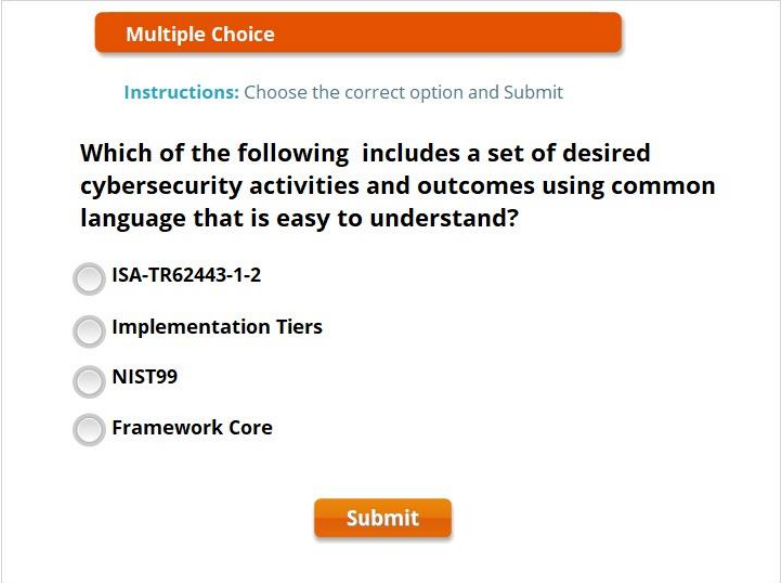
Correct	Choice
X	Radio Button 3



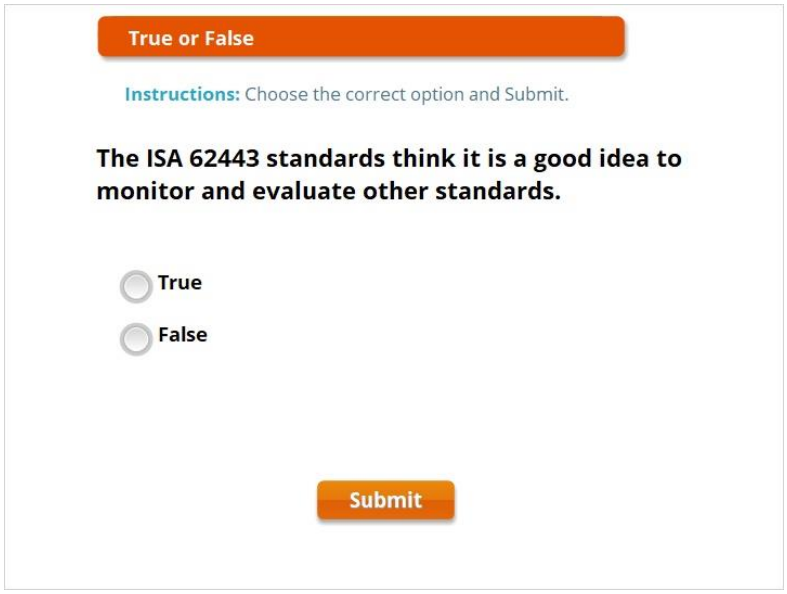
Correct	Choice
X	Radio Button 1



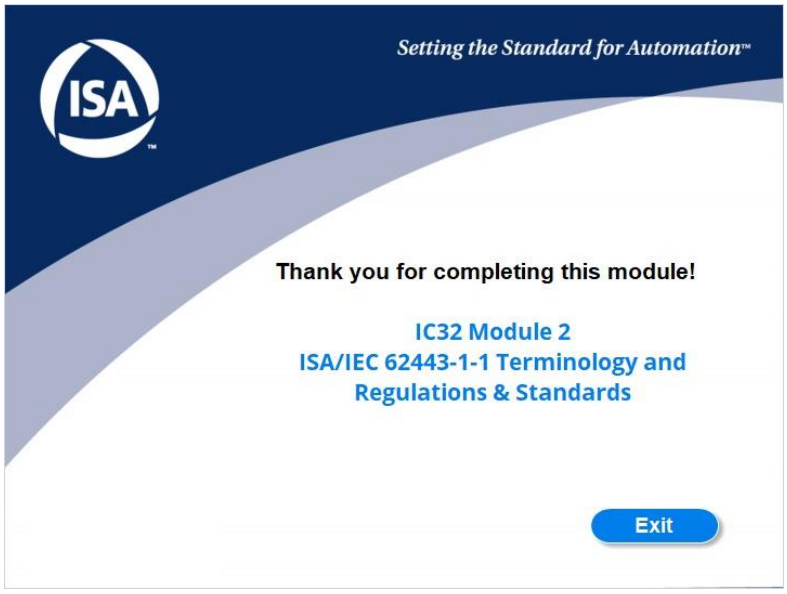
Correct	Choice
X	Radio Button 2



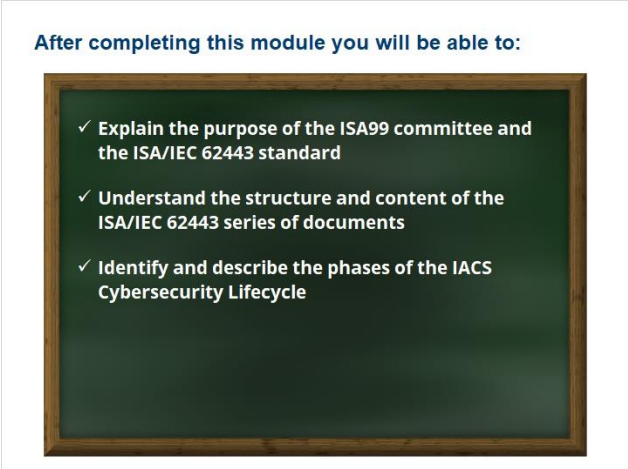
Correct	Choice
X	Radio Button 4



Correct	Choice
X	Radio Button 1



ISA IC329 Module 3



Notes:

- First let's take a bird's eye view of the committee from the outside.
- **Established in 2002** with a small handful of interested people has since grown to a membership of over 500 people
- These members come from virtually all industry sectors, although some are definitely more heavily represented than others.
- The focus of this group is not limited to any specific sector or industry type.
- We welcome membership, participation and contribution from anyone with interest and experience in the cybersecurity needs of their respective constituency.
- Also, our **membership is global**, consistent with the global reach and scope of the **International** Society of Automation (ISA).

Notes:

- The place to start is with an understanding of the scope that we defined for our efforts. This has remained essentially unchanged since the committee was formed.
- It was deliberately stated very broadly so as to provide a solid security context for a wide range of automation related areas.
- Such a broad scope is a result of the deliberate decision made by ISA in 2002 to form a single committee to address cybersecurity, rather than ask all other committees (existing and planned) to incorporate cybersecurity into their respective subjects. This approach has the benefit of being able to tap the knowledge of established cybersecurity experts, without requiring experts in other disciplines to become "min-experts" on what is often a very specialized and arcane subject.
- The scope definition is based primarily on an analysis of potential consequences, as shown here. Certainly cybersecurity failures are not the only potential source of these consequences, but they may be the least understood in the general engineering community.

Notes:

- That is the committee, but how does it operate? A full and detailed answer to this question is a complex subject itself, but one that is really only of interest to a smaller community of stakeholders, consisting of those who actively participate in committees.

- For our purpose today we will focus only on a few specific details that are important for our general stakeholders to understand.

Notes:

- To begin, let's spend a few minutes on the relationship between the ISA99 committee and committees and work groups of others **standards development organizations (SDO's).**
- In addition to ISA there are at least two other SDO's with an interest in the developing cybersecurity standards. The first of these is the International Electrotechnical Commission (IEC).
- When the ISA99 committee was formed there was an agreement between ISA and IEC to cooperate on the development of cybersecurity standards. This would avoid the need to create duplicate committees in each organization.
- As a result of this agreement the ISA99 committee is charged with developing the majority of the standards and practices in the 62443 series. These will be issued by ISA with numbers of the form ISA-62443-x-y.
- At the same time or shortly after the intent is for essentially the same standards to be issued by IEC with numbers of the form IEC-62443-x-y.
- Finally, the ISA99 committee is working closely with a joint technical committee (JTC) of ISA and IEC to ensure that our standards are consistent with the more general cybersecurity standards in the ISO-27000 series.
- These working partnerships can be complex and sometimes difficult, but the result is less duplication of effort, and ultimately less confusion and more consistency for the ultimate users of the standards.

Collaboration on Related Topics

- Process Safety (ISA84, IEC TC65)
- Wireless Communications (ISA100)
- Certification (ISCI and ISASecure®)
- Communications & Advocacy (Automation Federation)
- Security Framework (NIST)
- International Reach (IEC/ISO)

Notes:

- The ISA development and review process can easily take two years, with publication stretching out into the third year
- This is a good place to repeat that the numbering scheme has evolved since 2002
- The first edition of 62443-1-1 was published 2007 by IEC as a Technical Specification
- TR = Technical Report--informative publication, provides data or information on a particular technical subject.
- Not shown on this slide TS = Technical Specification-is just a level below an IEC International Standard.
    - It is generally developed when a full global consensus on a topic is too difficult to obtain within a useful time frame
- Only Standards contain “normative” content, clear and direct statements as to what shall be done

Notes:

- The work groups currently defined are shown
- So how does all of this come together as an organized effort?
- The ISA99 committee is organized as a series of work groups, each with a specific purpose within the context of the committee work plan.
- Work groups have chair(s) who are responsible for directing activity and reporting progress to the WG 5 committee leadership.
- In some cases work groups have been assigned responsibility for specific Work Products.
- In others the work group is focused on developing content that will be turn over to another group for publication.
- WG 6 - Patch Management (IEC/TR62443-2-3) done by IEC. The plan is for ISA to adopt it as an equivalent ISA-62443-2-3.
- Finally, there is a provision for the creation of work groups focused on aspects of committee operation (e.g., WG8)
- WG 10 was “shut down” with intent to “reactivate
    - ISA-TR62443-1-4: IACS security life-cycle and use cases may be assigned to WG10
    - Goal is to have a large “collection” of practical and useful use cases that address all aspects of the Lifecycle

WG 12 inactive for now; efforts to produce this document stalled; unable to identify the right number of contributors from approving countries in the IEC community (TC65 WG10)

ISA99 committee and the ISA/IEC 62443's (Cont'd)

- Once published as an IEC format
  - Pay to obtain the official publication
- PREFACE has listing of members and participants
- Subject Matter Experts (SME) in their area
- **Volunteering** their time and efforts
- It can take up to 3 years for a standard to be developed, reviewed, voted on and be published
- Always looking for new participants

Committee Participation

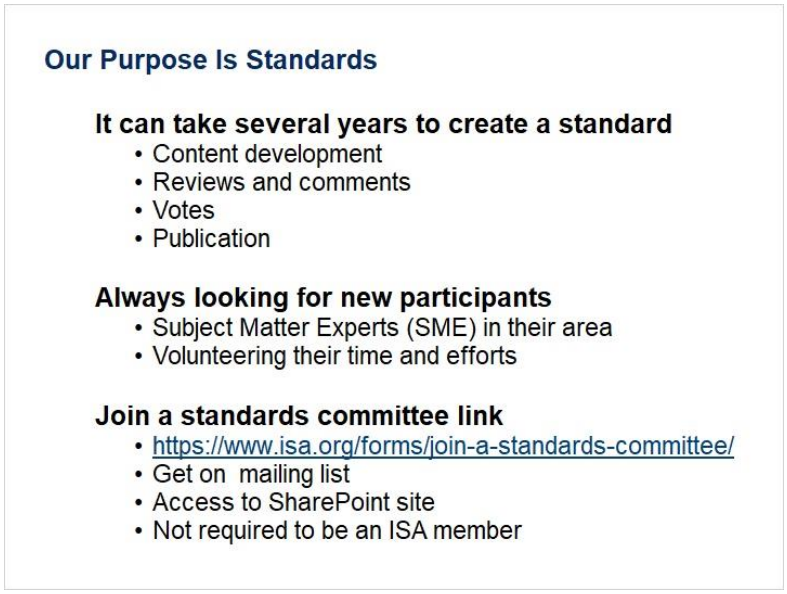
NOT necessary to be a member of ISA in order to be a member of an ISA committee

Membership Types

Type	Description
Information	• Default classification • Participates in one or more work or task groups • Comments on draft documents
Voting	• Maximum of one per company • Nominated based on contributions • Approved by existing voting members • Expected to vote on draft documents
Alternate	• Paired with a voting member • Able to vote if the primary voting member not available

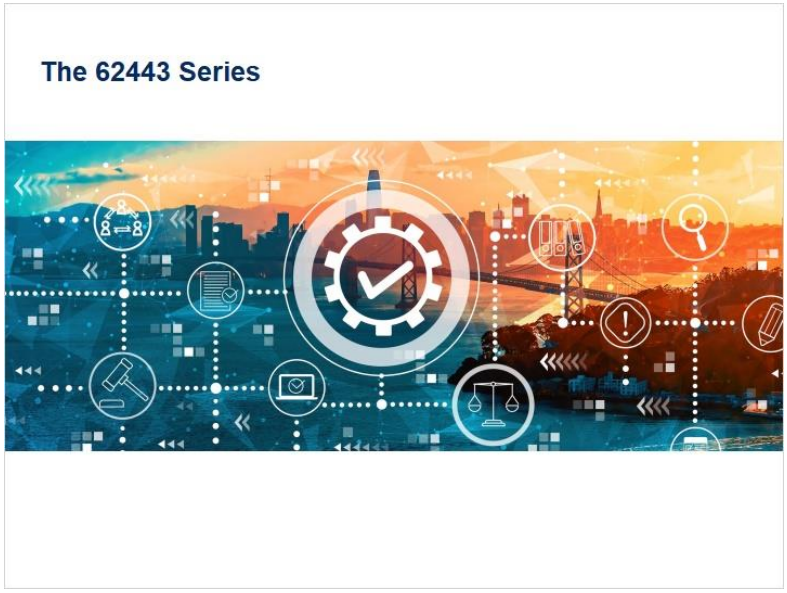
Notes:

- In addition to the previously mentioned formal relationships between standards development organizations (SDO's), the committee also maintains liaison relationships with several other committees and groups both within ISA and externally.
- In the case of other ISA committees, recall the decision to centralize the development of cybersecurity standards into a single committee. This requires that this committee work closely with the other committees to ensure that their perspectives and needs are adequately addressed. Examples of committees with which we have such relationships include ISA84 (process safety) and ISA100 (wireless communications).
- Within the Automation Federation we work closely with the Industrial Security Compliance Institute (ISCI) to ensure that the ISASecure certification program remains consistent with the contents of our standards.
- In addition to other ISA and the Automation Federation we also maintain relationships with external groups such as the Industrial Control Systems Joint Working Group (ICSJWG) and various sector-specific groups and government initiatives, such as the NIST Framework.
- As already described we maintain active relationships with IEC and ISO to ensure global adoption and consistency.



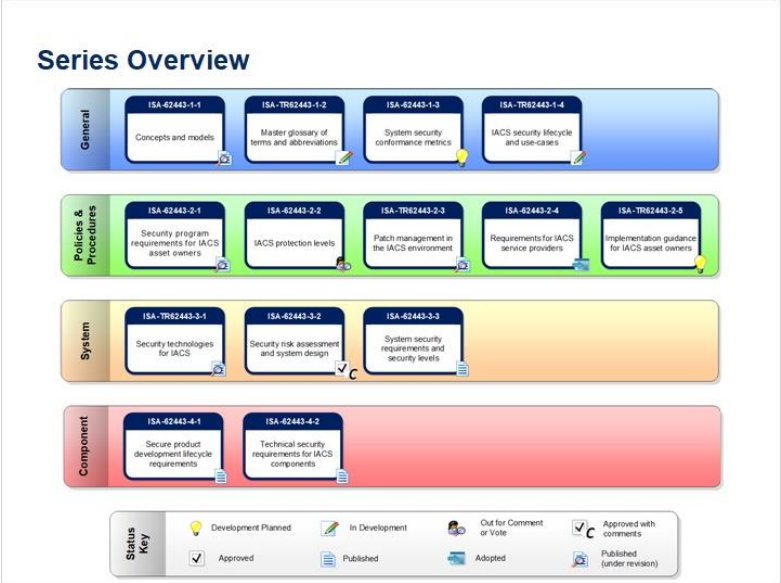
Notes:

- Finally, there is recognition that all of this cannot be done in a vacuum. Security is an attribute of the system, and one that has to be addressed with full consideration given to other attributes that are also important. Moreover, it crosses over into many other technical areas, in various different ways.
- There are **other groups working at sector, national and international levels** to develop standards and practices in this area.
- This is why it is important to stay abreast of what is going on and to form the necessary alliances and partnerships to remain relevant



Notes:

- All ISA committees are expect to produce some combination of Standards, Recommended Practices and Technical Reports, depending on the needs associated with the subject at hand.
- Of these only standards contain “normative” content, generally defined as including clear and direct statements as to what shall be done.
- The other two types of work products Recommended Practices and Technical Reports are generally considered to include only guidance information.



Notes:

- This graphic is used to show on a single page the full range of work products developed, in development or planned by the committee.
- As such, it provides perhaps the best “birds eye” view of what we have produced, and what we plan to produce in the future.
- The details of this organization change from time to time as circumstances dictate (e.g., the release of a completed standard).
- All such changes are reviewed and approved by a vote of the committee
- Currently there are 14 Publications
    - Over a thousand pages total
- The contents of each of these tiers or groups is described in a bit more detail in the next few slides
- Holistic approach works best-no standard is an island

Work Product Organization (Tiers)

First or top **General** tier contains standards and reports that are general in nature

Second tier **Policies & Procedures** addresses the people and process aspects of an effective security program

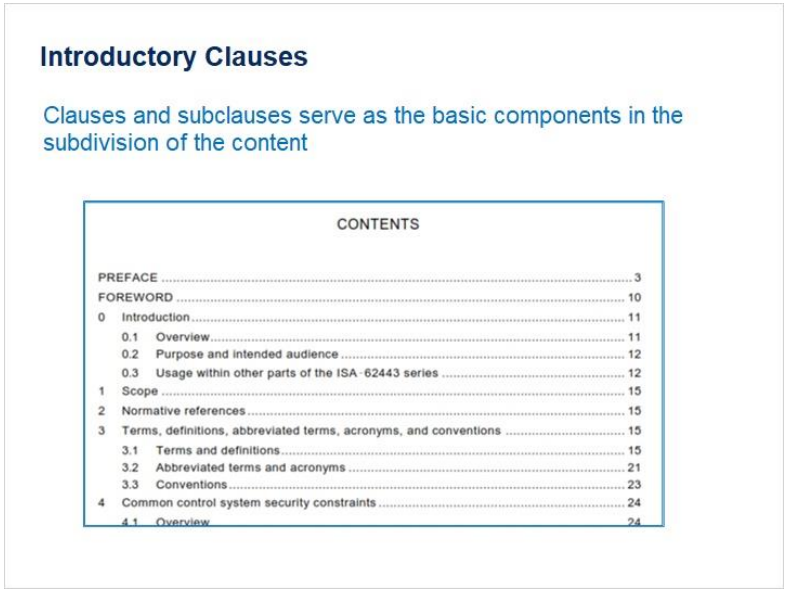
Third tier **System** focus is on the technology related aspects of security

Fourth tier **Component** focuses on specific security related technical requirements of products and components

- **Turning from defining what must be done**
- **To providing direction on how it should be accomplished**
- **Growing interest in measuring effectiveness and conformance**

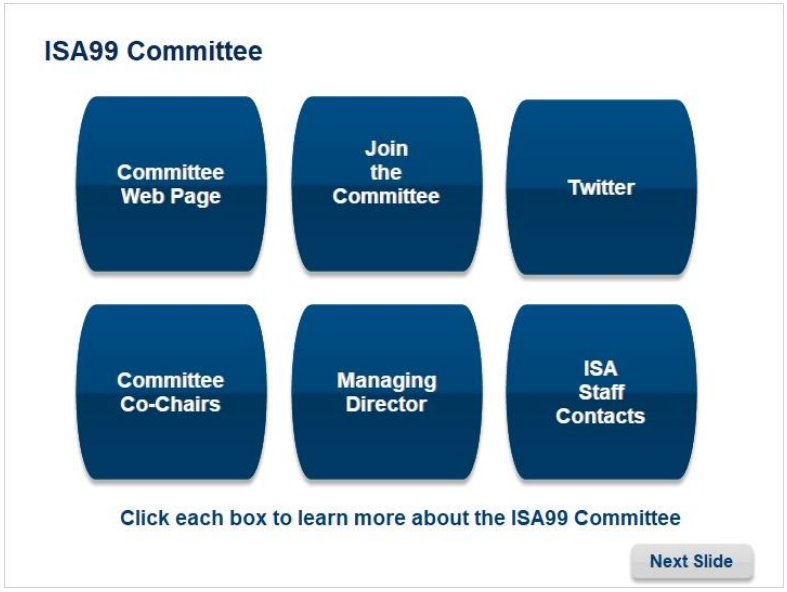
Notes:

- The first thing to note when looking at this diagram is that our work products are organized into **four distinct groups or tiers**, each with a specific focus
  - Note that the tiers may also be referred to as Main Series, Levels, Categories, Layers, Groups and even Zones in various publications
  - We shall try to use groups or tiers for consistency
  - Across the tier the standards are also referenced as Part 1-1, Part 1-2, Part 1-3, Part 1-4,
- The first group or top tier contains standards and reports that are general in nature, and must be understood by the entire stakeholder community in order to successfully apply the standards.
- With these general subjects established we move on to the second tier, which addresses the people and process aspects of an effective security program. The audience for these documents includes people who develop and operate these programs across the entire Lifecycle of solutions.
- With the general concepts and process related aspects addressed we move to the third tier, where the focus is on the technology related aspects of security. This includes both an assessment of available technologies and their suitability for use in this context, as well as the specific requirements related to the technical aspects of a security program.
- Finally, the fourth tier focuses on the specific security related technical requirements of the products and components that are used to assemble industrial control systems.
- By now you have probably observed that the second field of the numbering scheme aligns with the tier or group

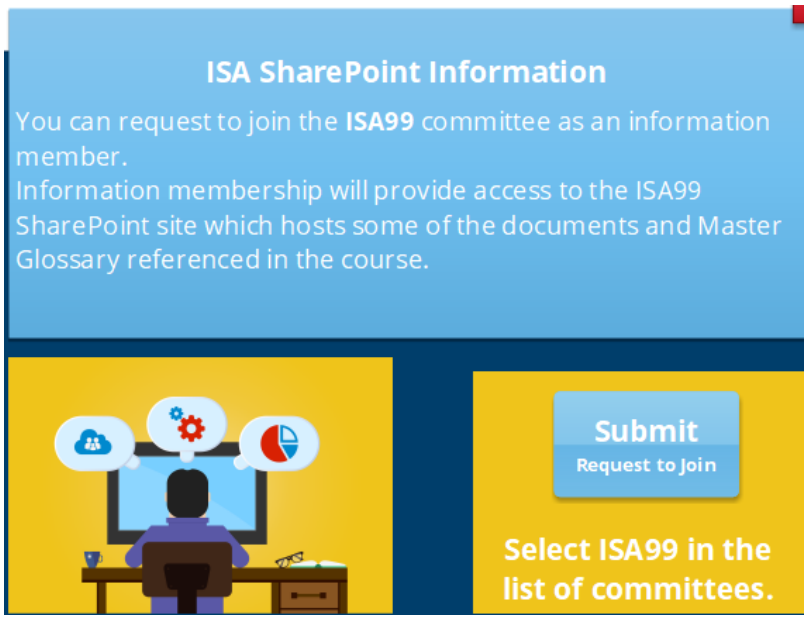


Notes:

- Clauses and subclauses serve as the basic components in the subdivision of the content of a document.
- Example-- Clause 0 Introduction, Subclause 0.1 or Clause 3, Subclause 3.1 etc…
- http://www.iec.ch/standardsdev/resources/draftingpublications/directives/subdivision/
- http://www.iec.ch/standardsdev/resources/draftingpublications/directives/components/

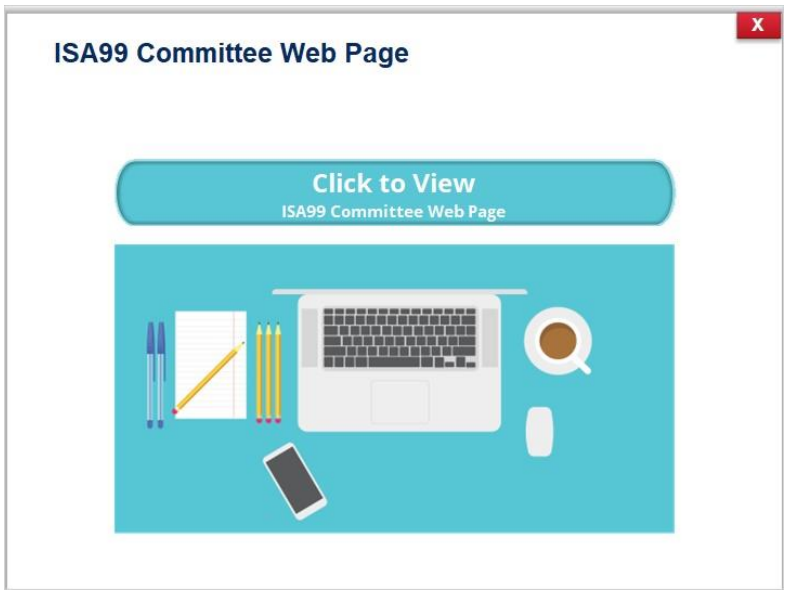


Join Committee



https://www.isa.org/forms/join-a-standards-committee/

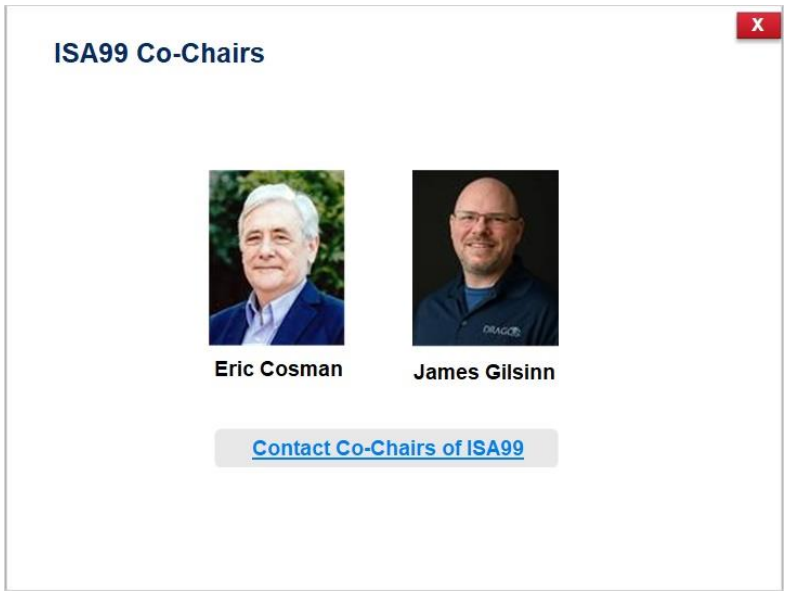
Committee Web Page



https://www.isa.org/ISA99/

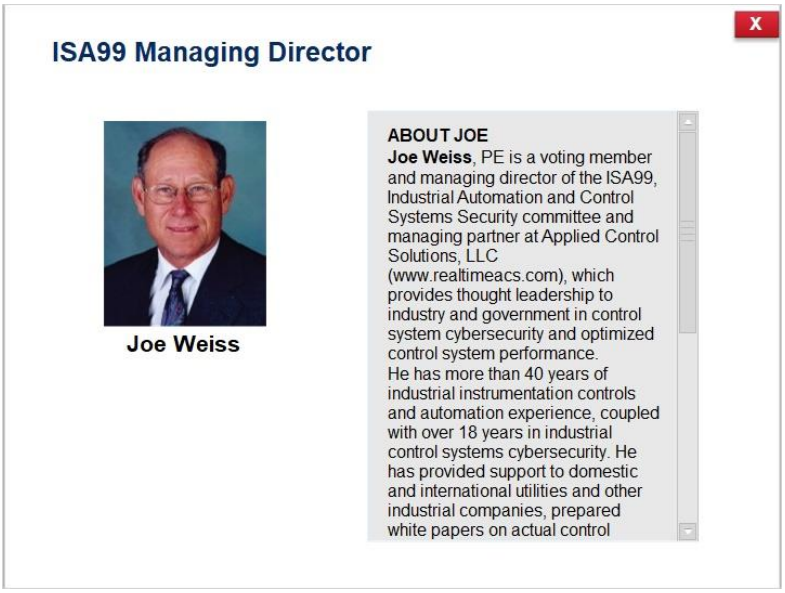
Twitter

Committee Co-Chairs

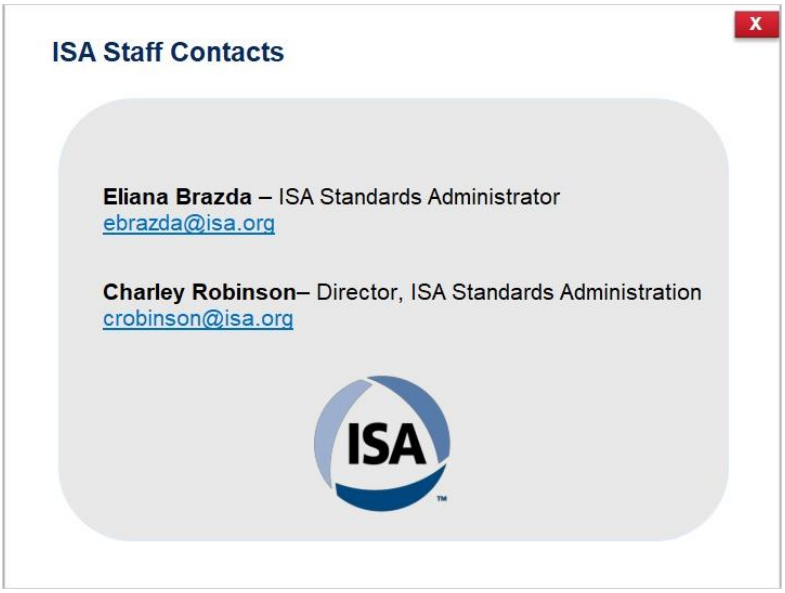


ISAChair@gmail.com

Managing Director



ISA Staff Contacts



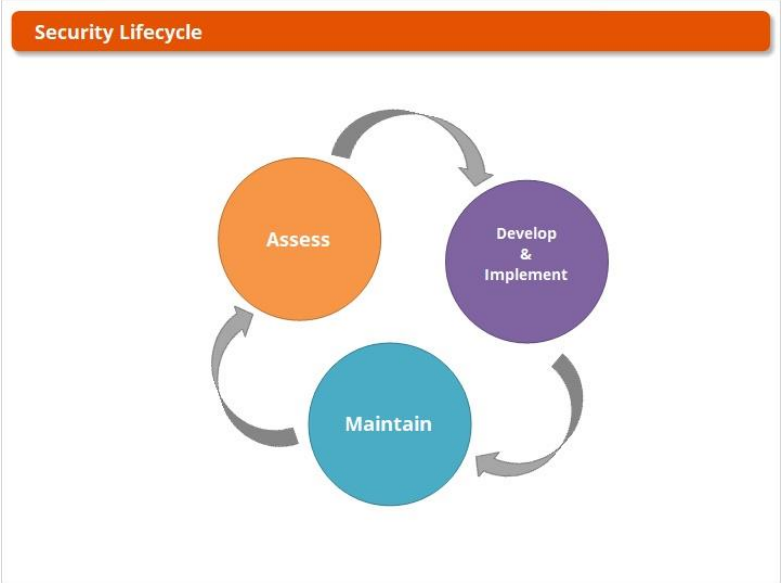
ISA99 committee and the ISA/IEC 62443's (Cont'd)

- ✓ Review…..
- ✓ Who are we?
- ✓ How do we work?
- ✓ What are the basics?
- ✓ What are our work products?
- ✓ Where do things stand?

Notes:

- In review, we have seen an overview of the ISA99 committee and its current and planned work products
- In closing this section out remember "The Only Thing That Is Constant Is Change -"
    - Quote attributed to Heraclitus of Ephesus (c.535 - c.475 BCE) a pre-Socratic Greek philosopher,

Intro to IACS Cybersecurity Lifecycle



Notes:

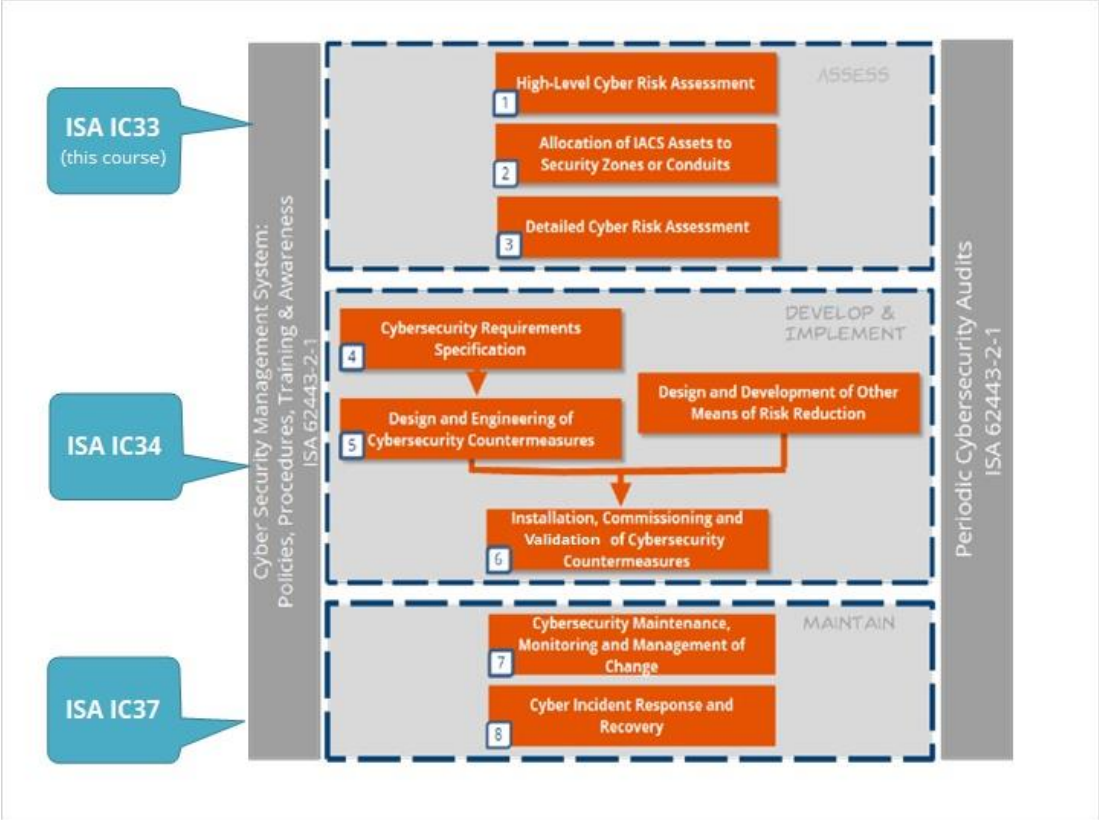
The security life cycle in the ISA 62443 Standard includes three phases:

· Assess

· Develop and Implement

· Maintain

The security lifecycle is a continuous process needed to minimize risks.



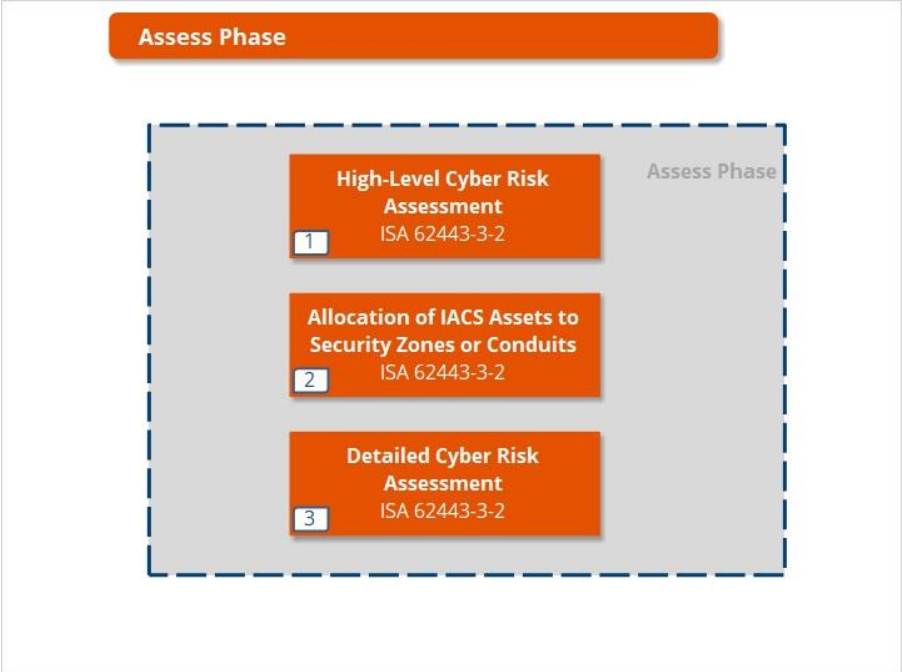
Notes:

ISA's Cybersecurity Training series includes courses which address all 3 phases of the cybersecurity lifecycle.

This course, IC 33, covers information relating to the assess phase.

IC34 provides students with knowledge and skills needed in the develop and implement phase.

And IC37 includes topics related to the maintain phase.



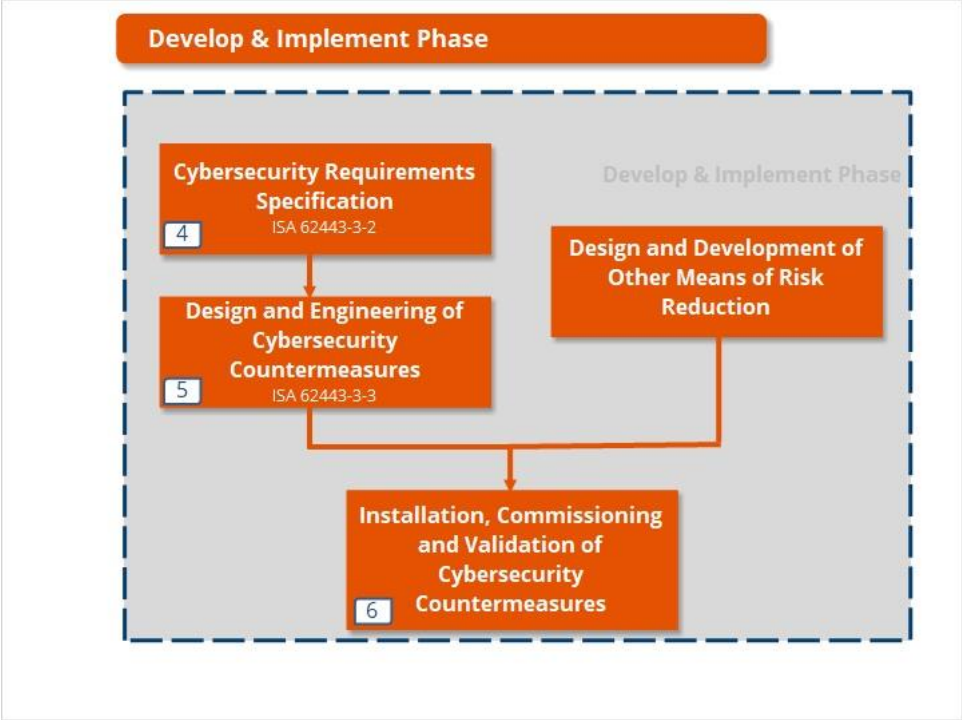
Notes:

In the Assess phase,

Topics include:

- High-Level Cyber Risk Assessment.
- Allocation of IACS Assets to security zones or conduits.
- Detailed Cyber Risk Assessment.

ISA Standard 62443-3-2 provides guidelines for the Assess phase.



Notes:

Let's take a closer look at the Development and Implementation phase.

Topics include:

• Cybersecurity Requirements Specification,

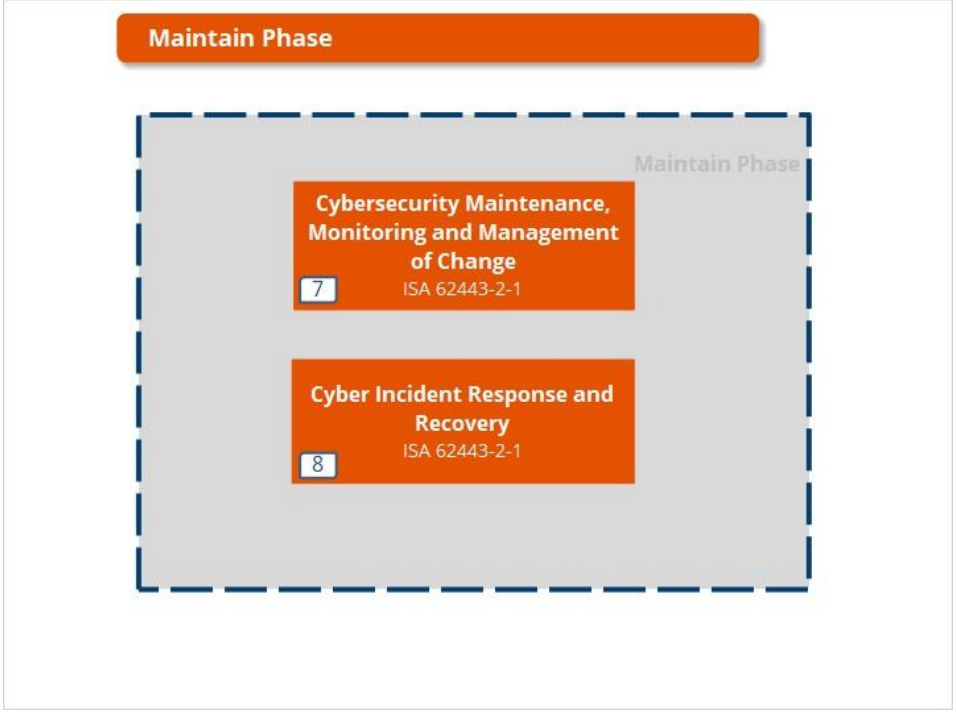
• the design and engineering of cybersecurity countermeasures.

And

• the installation, commissioning, and validation of cybersecurity countermeasures

ISA Standard 62443-3-2 and 3-3 provides guidelines for the development and implementation phase.

The design and development of other means of risk reduction may also be included.

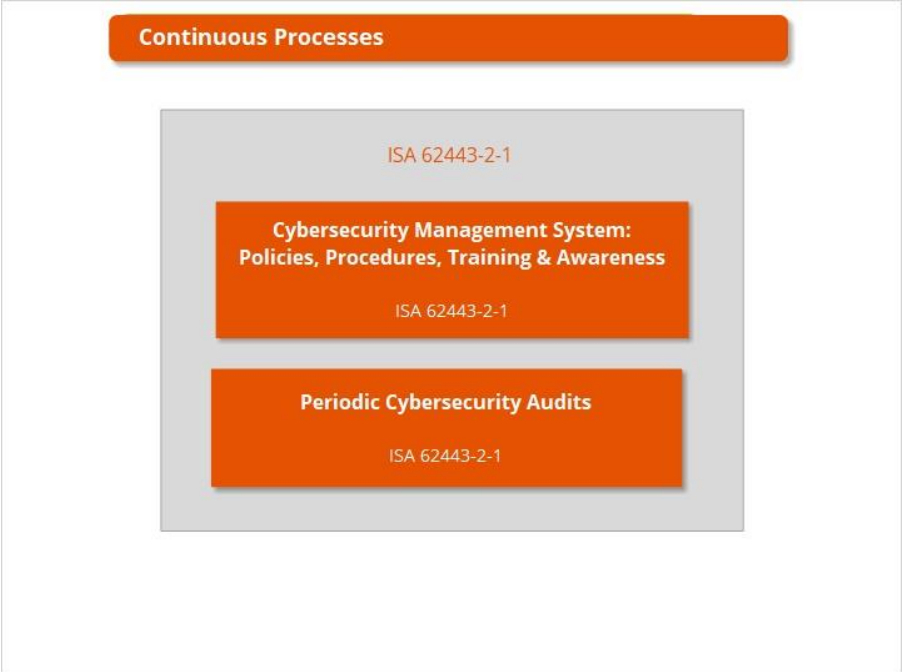


Notes:

The maintain phase in the cybersecurity lifecycle includes:

Cybersecurity countermeasures Maintenance, monitoring and change management.

as well as Incident Response and Recovery. ISA standard 62443-2-1 addresses cybersecurity maintenance.



Notes:

I. S. A. standard 62443-2-1 also provides guidelines for processes which should be continuously monitored.

This includes a cybersecurity management system for:

· Policies

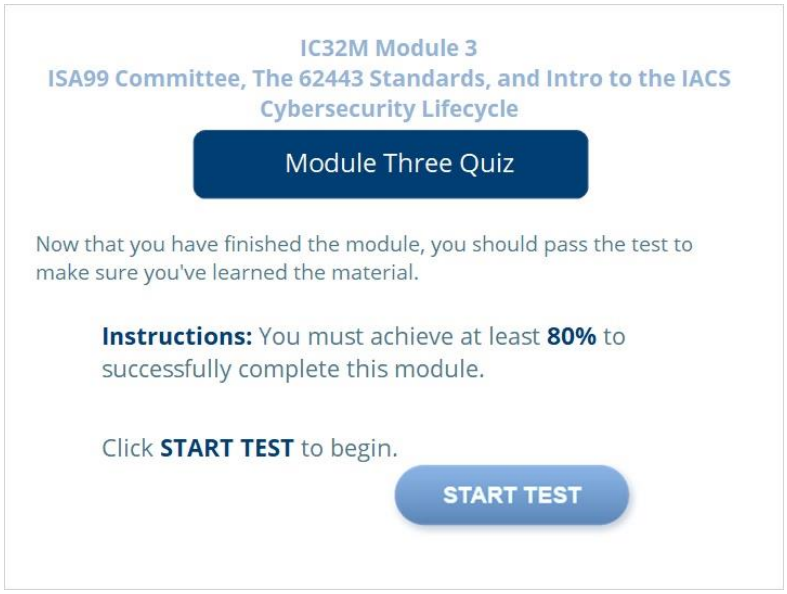
· Procedures

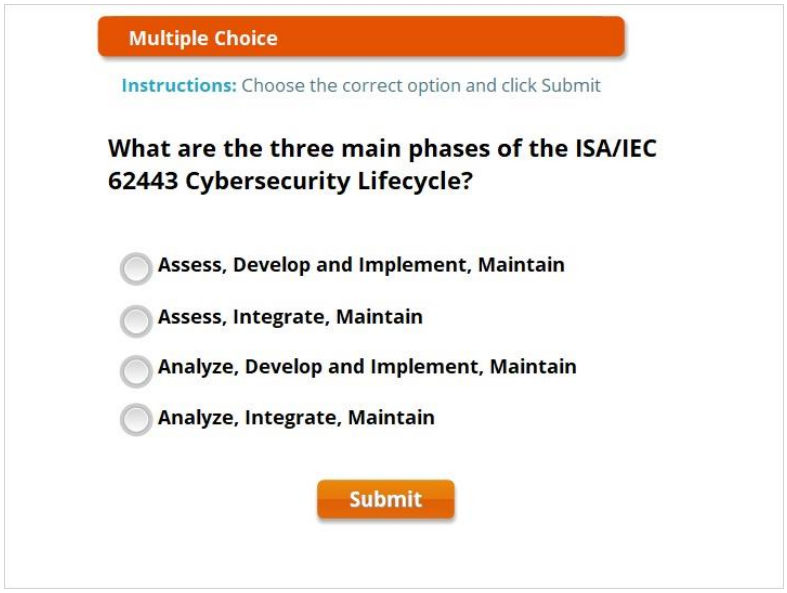
· Training

· Awareness

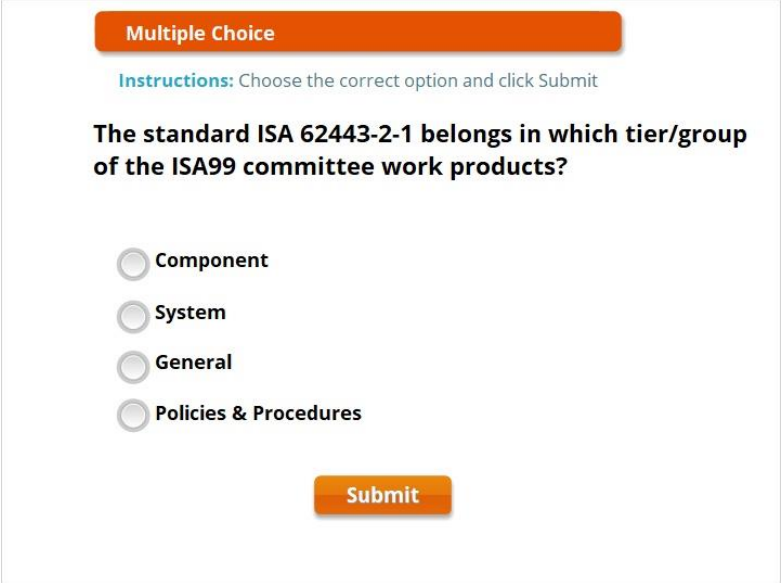
Periodic Cybersecurity audits should also be conducted as a continuous process.

Drag Item	Drop Target
Assess Phase	3
Develop & Implement Phase	2
Maintain Phase	1

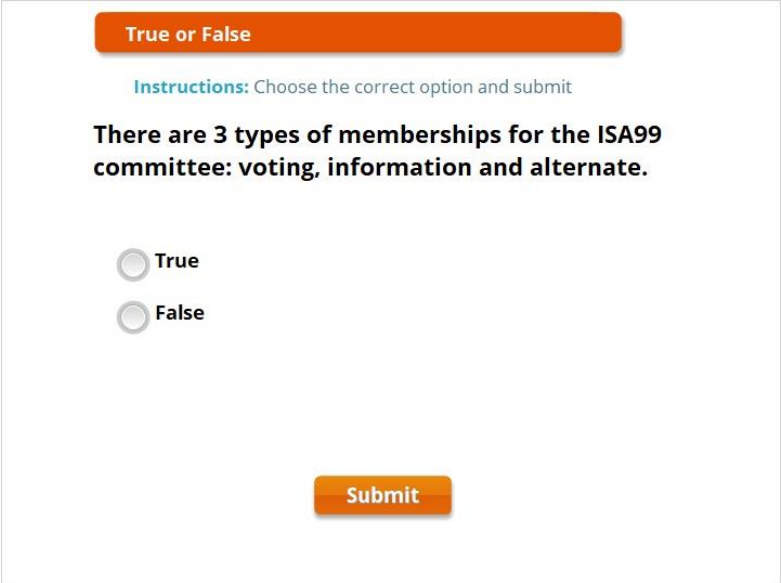




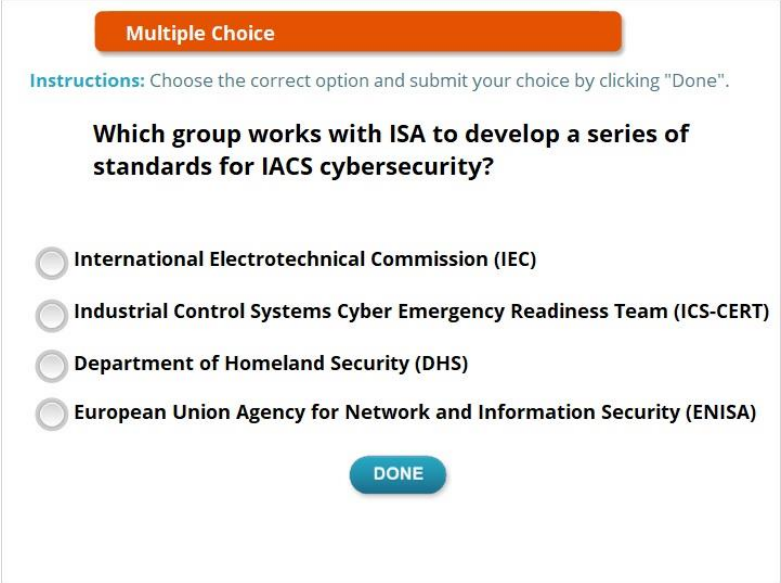
Correct	Choice
X	Radio Button 1



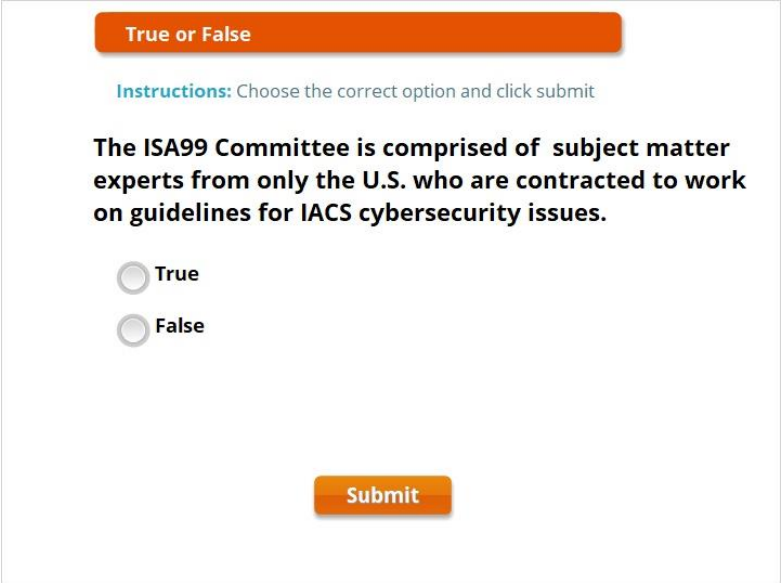
Correct	Choice
X	Radio Button 4



Correct	Choice
X	Radio Button 1



Correct	Choice
X	Radio Button 1



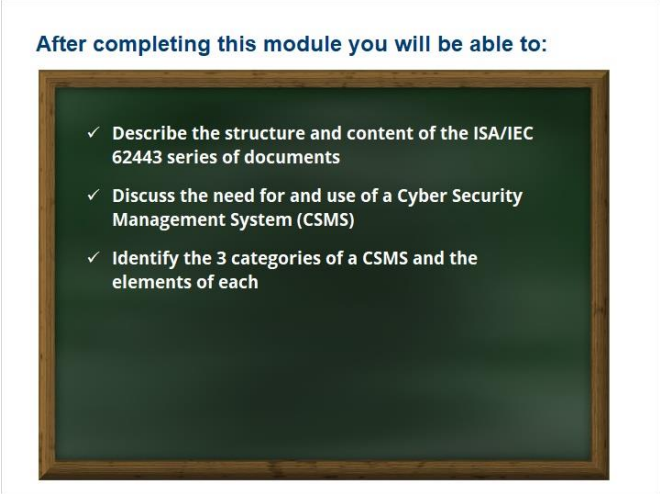
Correct	Choice
X	Radio Button 2

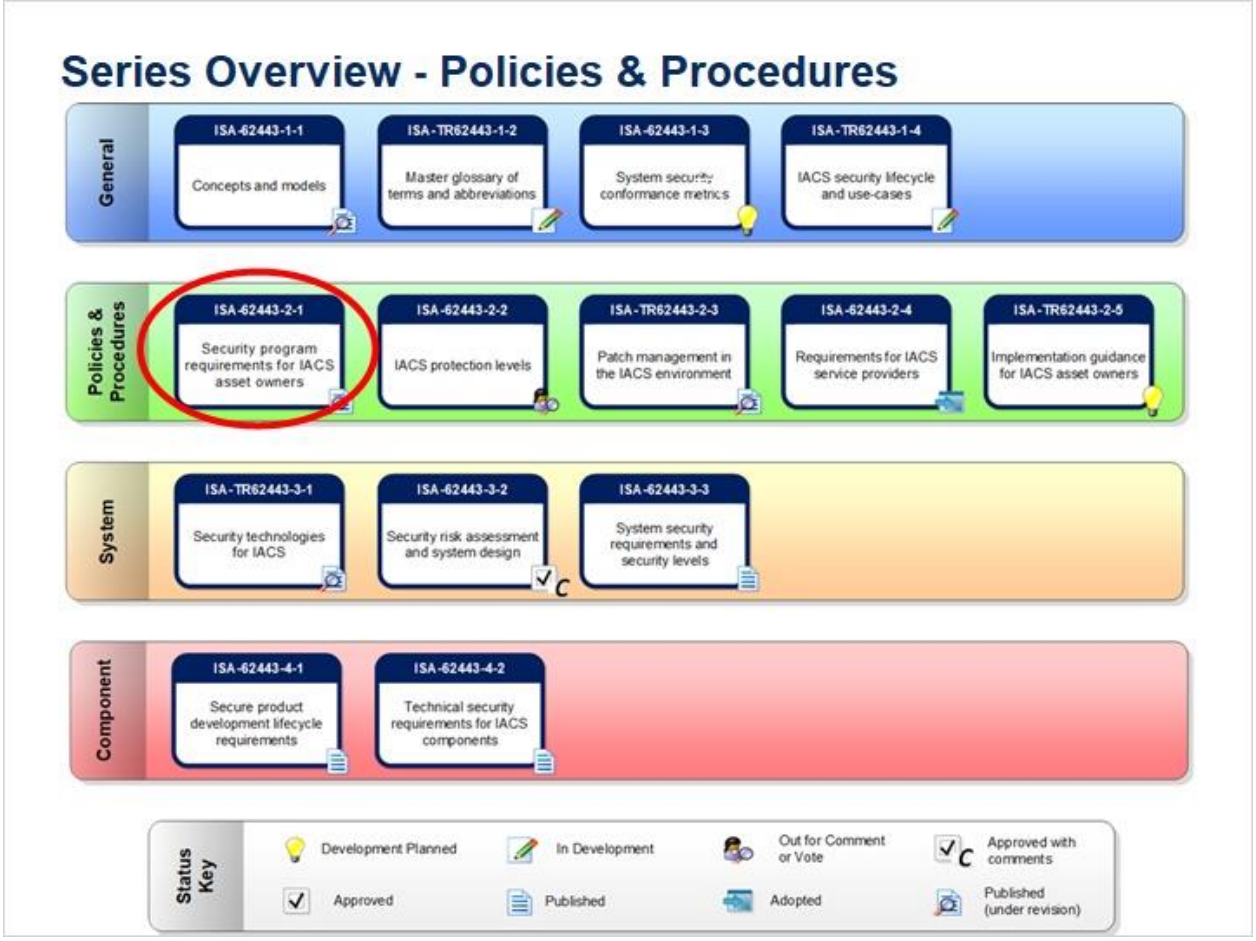

Setting the Standard for Automation™
Thank you for completing this module!
Module Three:
ISA99 Committee, The 62443 Standards, and Intro to the IACS Cybersecurity Lifecycle
Exit

Week 3

Setting the Standard for Automation™

ISA IC329 Module 4

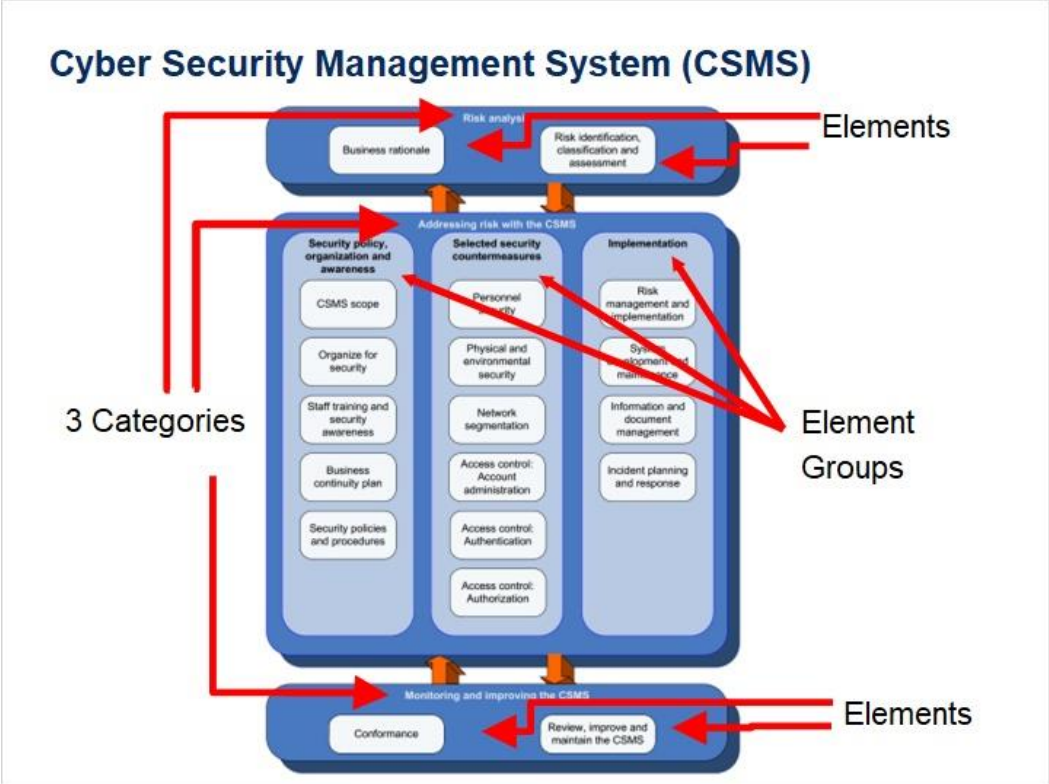




Notes:

- 62443-2-1 Requirements for an IACS Security Management System
    - aka Security for Industrial Automation and Control Systems: Establishing an

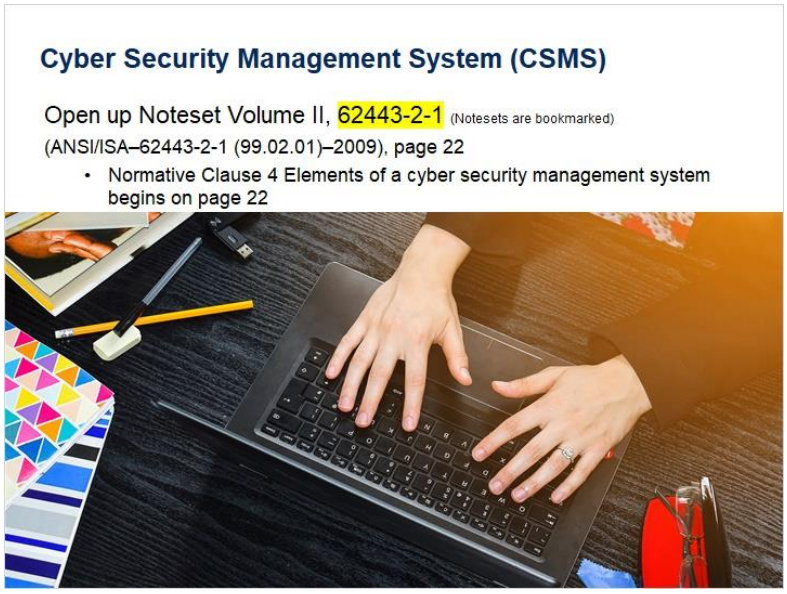
Industrial Automation and Control Systems Security Program
    - **See Noteset Volume II, 62443-2-1 for current copy (ANSI/ISA-62443-2-1 (99.02.01)-2009)**
    - Review in progress to improve alignment with ISO 27001:2013
- TR62443-2-2 (not included with Noteset Volume II)
    - Implementation Guidance for an IACS Security Management System (D1 E4 April 2013) proposed
    - This proposed technical report will build on the content of ISA-62443-2-1
    - Focusing on the operation of a security management system
    - There will be strong alignment with the ISO 27000 series of standards.
- TR62443-2-3 Patch management in the IACS environment (not included with Noteset Volume II) Published July 2015
- 62443-2-4 Security program requirements for IACS service providers (not included with Noteset Volume II)
    - Published by IEC in 2015
    - WG10 of IEC Technical Committee (TC) 65
    - Proposed adoption by ISA
- http://isa99.isa.org/ISA99%20Wiki/Home.aspx (Retrieved 16 November 2016)
- How do we go about Establishing an Industrial Automation and Control Systems Security Program?
- One approach is to develop a Cyber Security Management System (CSMS)



Notes:

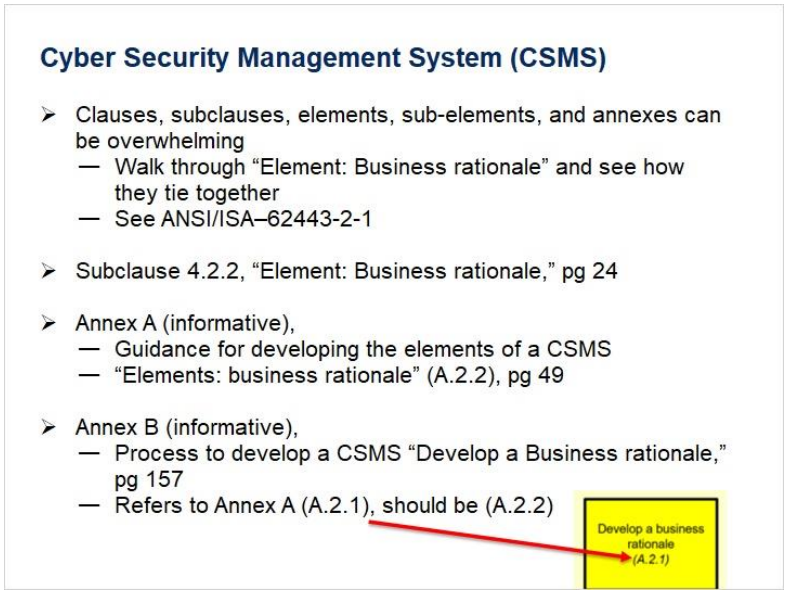
- Overview of CSMS
- **Developing CSMS is a journey that may take months or years to achieve and it is a continuous process**
    - **You are never done**
- This slide points out categories, elements, element groups
- In the next few slides we will list each of the categories
- We will then go through the process of creating a CSMS
- Refer to Noteset Volume II Additional Resources tab for a handy full page copy of the CSMS graphic
- Across the 62443's there is not perfect alignment with terms and references
    - You have to deal with it just like any other standards or guidelines
    - Alignment and changes during development and publication may have been missed or typos occur
    - "Search/find" is useful tool for researching a topic and references
    - As standards are reviewed there is a concerted effort to update alignment
- Use of the element or sub-element number is also intended to provide the instructor a reference to take a deeper dive if time allows

2.9 Cyber Security Management System (CSMS)



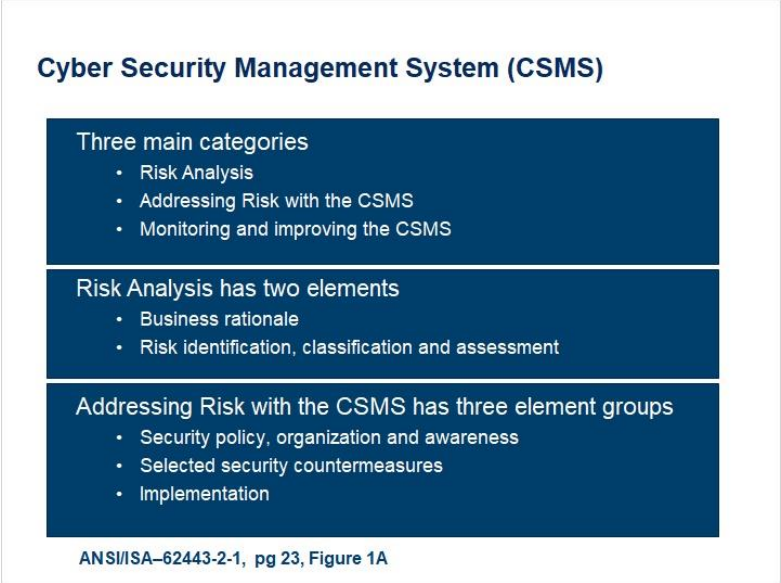
Notes:

- Overview of CSMS
- It is important to get familiar with the layout of the standards to get the full benefit of the informative Annexes
- Have students open up Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), page 22.
    - Note normative Clause 4 Elements of a cyber security management system begins on page 22.
    - Figure 1, page 23 is the graphical view of elements of a cyber security managment system
    - Annex A, page 47 is an informative Guidance for developing the elements of a CSMS
    - Annex B, page 155 is an informative Process to develop a CSMS starting on page 155.
    - Annex B is the process we will go through in more detail.
- IMPORTANT NOTE regarding Annex B starting on page 155
    - Where applicable there is a reference to Annex A within the boxes (e.g. (A.2.2, pg. 49))
    - The published ISA standard references in Annex B are out of alignment with Annex A
    - The corrected (best effort) references have been updated on this slide set
    - Recommend students note reference discrepancy in their hardcopy noteset



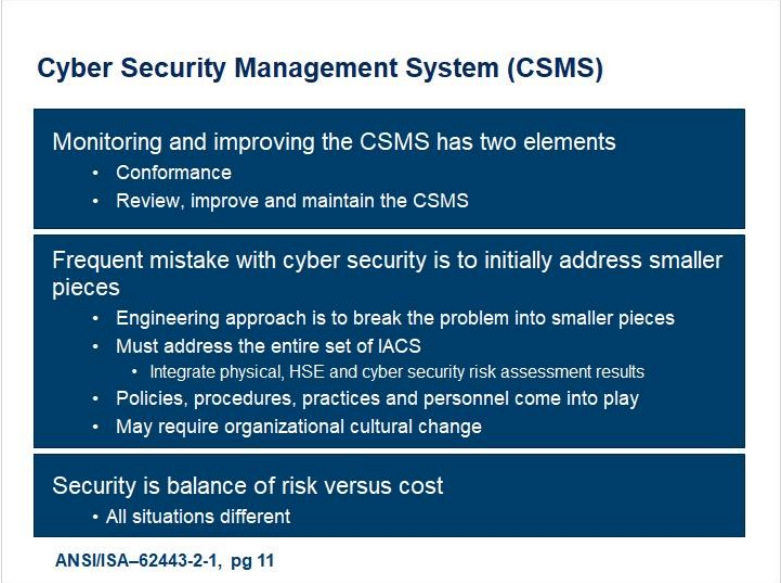
Notes:

- Overview of CSMS
- The clauses, elements, sub-elements and Annexes can be overwhelming at first so breaking them down at this point may be helpful
- Have students open up Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009),
- Example
    - Clause 4.2.2, "Element: Business rationale" is on page 24
    - Annex A informative guidance "Elements: business rationale" (A.2.2) is on page 49
    - Annex B step "Develop a Business rationale" is on page 157
- IMPORTANT NOTE regarding Annex B starting on page 155
    - Where applicable there is a reference to Annex A within the boxes (e.g. (A.2.2, pg. 49))
    - The published ISA standard references in Annex B are out of alignment with Annex A
    - The corrected (best effort) references have been updated on this slide set
    - Recommend students note and reference discrepancy in their noteset



Notes:

- Refer to Additional Resources tab for a copy of the CSMS graphic
- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), page 23, Figure 1



Notes:

- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), page 11
- HSE = Health, Safety and Environmental

Cyber Security Management System (CSMS)

IACS risk may have unrecoverable consequence
- Business risk may only be temporary financial setback
- Control HSE consequences may be permanent

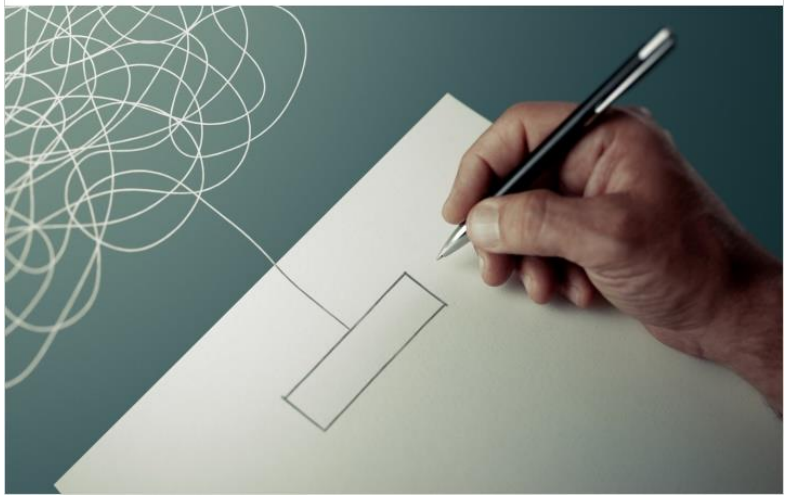
Cookbook approach using mandatory security practices
- Overly restrictive and costly
- Insufficient to realistically address the risk
- Not a one-size-fits-all set of security practices exists

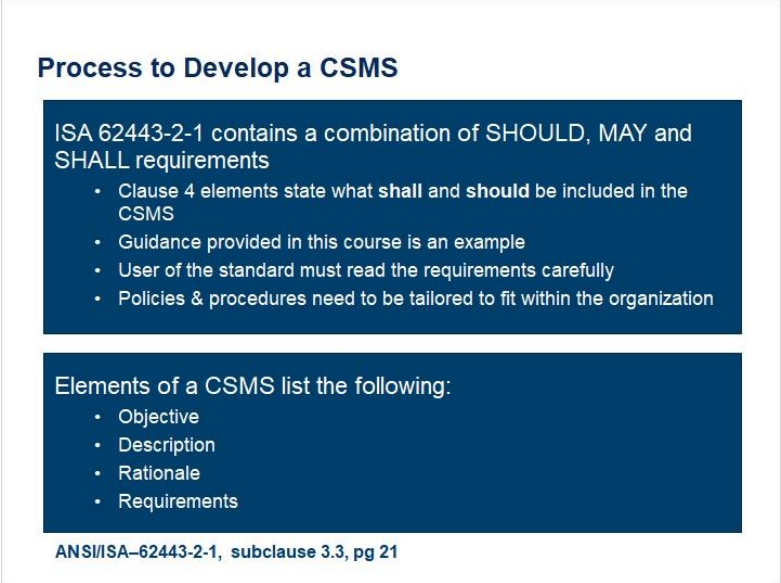
ANSI/ISA–62443-2-1, pg 11

Notes:

- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), page 11
- HSE = Health, Safety and Environmental

Process to Develop a CSMS



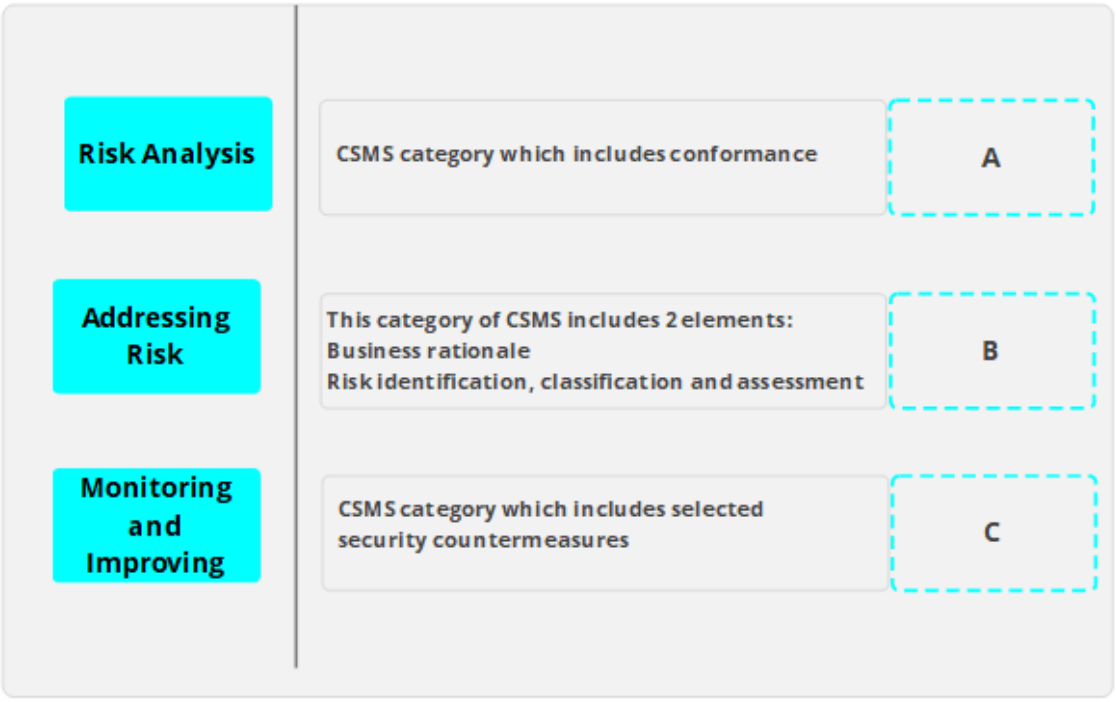


Notes:

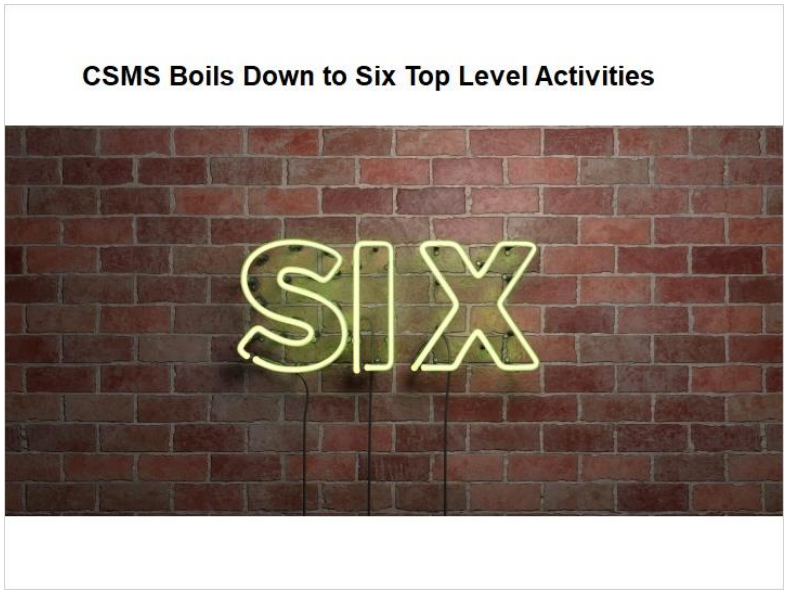
- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), Clause 3.3, page 21
- Page 25 has first requirement depicted as a table
- Requirements are presented as a table but not treated as tables
- The tables list the descriptions and the requirements for these elements,
- Description numbered similar to a sub-clause.
- Note that the tables are not referenced with table numbers
- The reference is given by the heading number in the description cell of the table

Knowledge Check

Drag each CSMS category to its matching description.

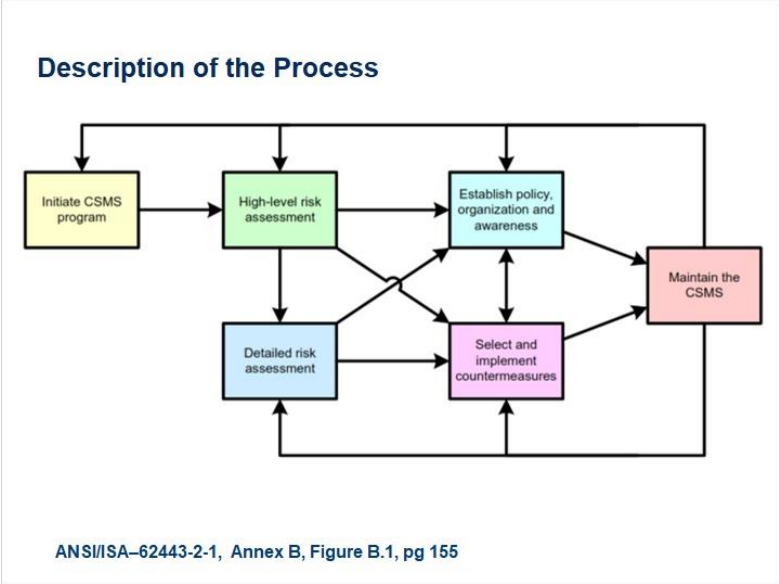


Drag Item	Drop Target
Risk Analysis	B
Addressing Risk	C
Monitoring and Improving	A



Notes:

- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), Annex B, page 155
- CSMS boils down to six top level activities



Notes:

- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), Annex B, Figure B.1, page 155
- CSMS boils down to six top level activities
- We shall first introduce each activity and then drill down to get a better understanding of each activity
- Going from left to right note the iterative process(es)
- Also note iterative and branching processes within the steps
- "rinse, lather and repeat"
- We will identify common pitfalls that can hinder success
- Reminder---IMPORTANT NOTE regarding Annex B starting on page 155
    - Where applicable there is a reference to Annex A within the boxes (e.g. (A.2.2, pg. 49))
    - The published references in Annex B are out of alignment with Annex A
    - The corrected (best effort) references have been updated on this slide set

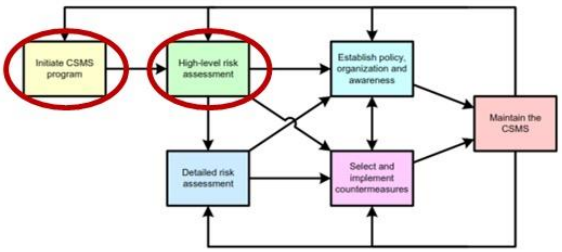
Description of the Process (Cont'd)

Initiate CSMS

- ✓ Establish purpose
- ✓ Organizational support
- ✓ Resources
- ✓ Scope
  - Initial scope may be smaller than desired
  - Can grow as the program matures

High-level risk assessment

- ✓ Drives the content of CSMS
- ✓ Threats
- ✓ Likelihood
- ✓ Vulnerabilities
- ✓ Consequences



Notes:

- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), Annex B.2
- Initial scope may be smaller than desired but can grow as the program matures
- Don't try to eat the whole elephant at one time

Description of the Process (Cont'd)

Address risk assessment at a high level

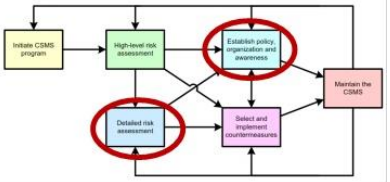
- ✓ Resources needlessly expended if not kept high level
- ✓ Overall higher level risk context has to be established

Detailed risk assessment

- ✓ Detailed technical assessment
- ✓ Focus on vulnerabilities identified at high level

Establish policy, organization and awareness

- ✓ Driven by high-level and details risk assessment results
- ✓ Creation of policies and procedures
- ✓ Assignment of organizational responsibilities
- ✓ Planning and execution of training



Notes:

- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), Annex B.2

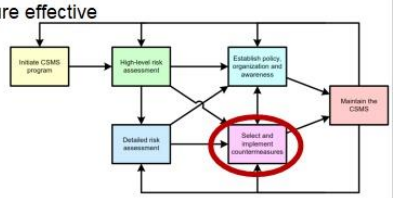
Description of the Process (Cont'd)

Select and implement countermeasures

- ✓ Defines and implements cybersecurity defenses
- ✓ Technical
- ✓ Non-technical

Coordinated approach

- ✓ High-level and low-level decisions driven by risk assessment results
- ✓ Establish policy, organization and awareness
- ✓ Select and implement countermeasures
- ✓ Training
- ✓ Essential to make countermeasure effective



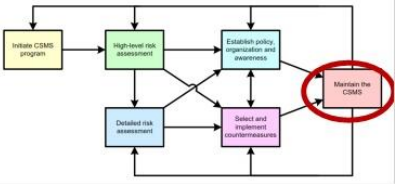
Notes:

- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), Annex B.2

Description of the Process (Cont'd)

Maintain the CSMS

- ✓ Is organization maturing in its CSMS activities?
- ✓ Does organization conform to policies and procedures?
- ✓ Are cybersecurity goals met effectively?
- ✓ Do the goals need to change in light of internal or external events?
- ✓ Is a review of high-level or detailed risk assessment required?
- ✓ Are there improvements identified and implemented?
- ✓ Are there training enhancements to make?
- ✓ Has enthusiasm and support waned?
- ✓ Have other priorities pushed CSMS to the back burner?



Notes:

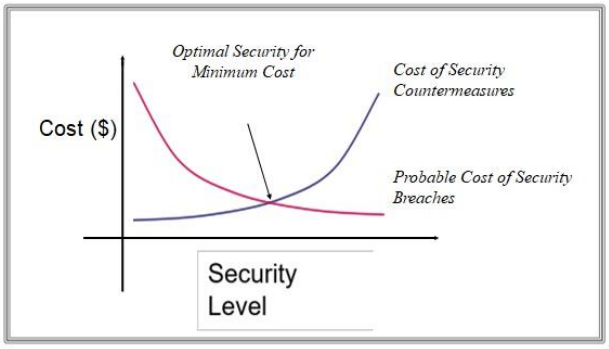
- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), Annex B.2
- Let's take a deeper dive into each of the six top level activities

Description of the Process (Cont'd)

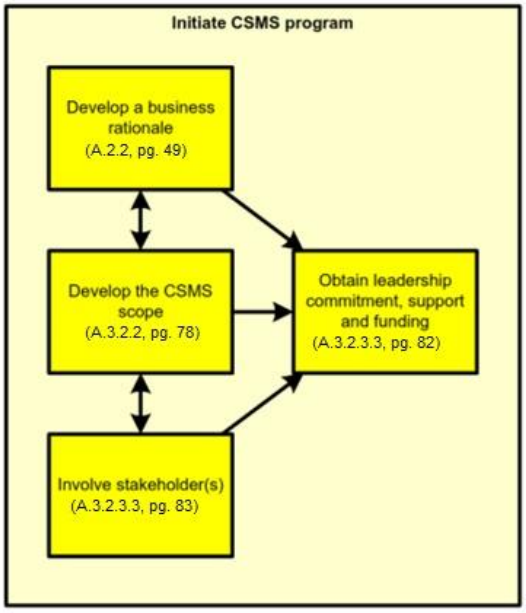
Fine balance

We can't afford perfect security

Risk reduction is balanced against the cost of security measures to mitigate the risk



Initiate the CSMS Program



ANSI/ISA–62443-2-1, Fig B.2, pg 157

- Reference Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009)

Notes:

- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), Annex B.2
- Do not make the business rationale sound like the sky is falling
- Senior management wants to see the hard numbers and reasoning backed up up with solid evidence from your risk assessment
- Finding the right metrics is not a trivial task

Initiate the CSMS Program (Cont'd)

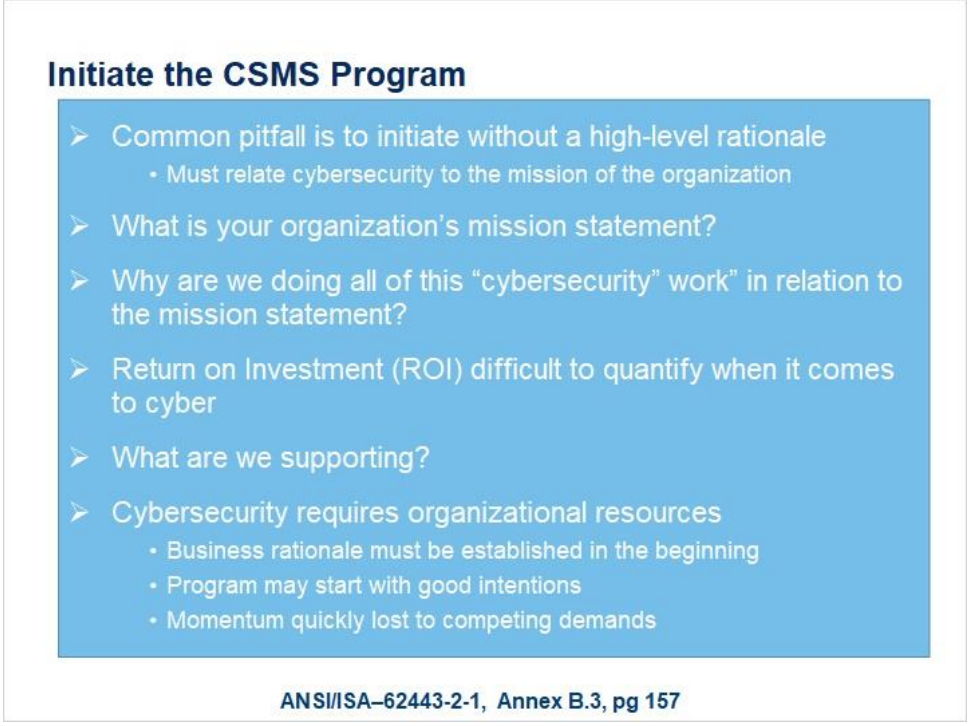
Stakeholders should be cross-functional in nature:

- ✓ Process control staff implementing/supporting IACS devices
- ✓ Operations staff responsible for making the product
- ✓ Safety management staff responsible for health, safety, and environmental incident prevention
- ✓ IT responsible for network and server design and support
- ✓ Physical security staff
- ✓ IT Security staff responsible for IT security
- ✓ Additional resources may be needed
  - legal
  - human resources
  - customer support roles
  - order fulfillment roles
  - vendors
  - third party contractors

ANSI/ISA–62443-2-1, Annex B.3, pg 157

Notes:

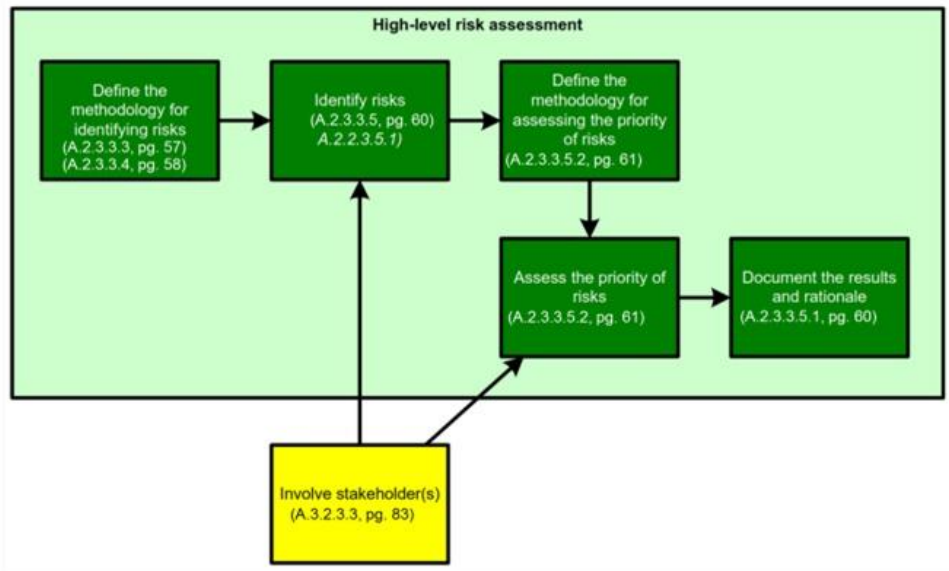
- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), Annex B.2
- Do not make the business rationale sound like the sky is falling
- Senior management wants to see the hard numbers and reasoning backed up up with solid evidence from your risk assessment
- Finding the right metrics is not a trivial task
- Identify all stakeholders (including employees, contract employees, and third-party contractors)



Notes:

- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), Annex B.2

High-level Risk Assessment



ANSI/ISA–62443-2-1, Fig B.3, pg 158

- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), Annex B.2

High-level Risk Assessment (Cont'd)

- Involves selecting methodologies for identifying and prioritizing risks and then executing those methodologies
- It is important to define these methodologies up front so that they will provide structure for the rest of the risk assessment
- Important to involve the stakeholders identified during Initiate step
- Common pitfall is to immediately jump into detailed risk assessment
  - Easy to do, especially with technical stakeholders
  - Avoid the "shiny object syndrome"

ANSI/ISA–62443-2-1, Annex B.4, pg 158

Notes:

- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), Annex B.2

High-level Risk Assessment (Cont'd)

- Documenting the results and rationale is important
  - Documentation establishes baseline
  - Will be found invaluable when the risk assessment needs to be confirmed or updated in the future
- Common pitfall documentation is insufficient or never completed
  - There needs to be a champion appointed for good follow up

ANSI/ISA–62443-2-1, Annex B.4, pg 158

High-level Risk Assessment (Cont'd)

- Thresholds for tolerable risk are established by executive management
- Often communicated via a Risk Matrix

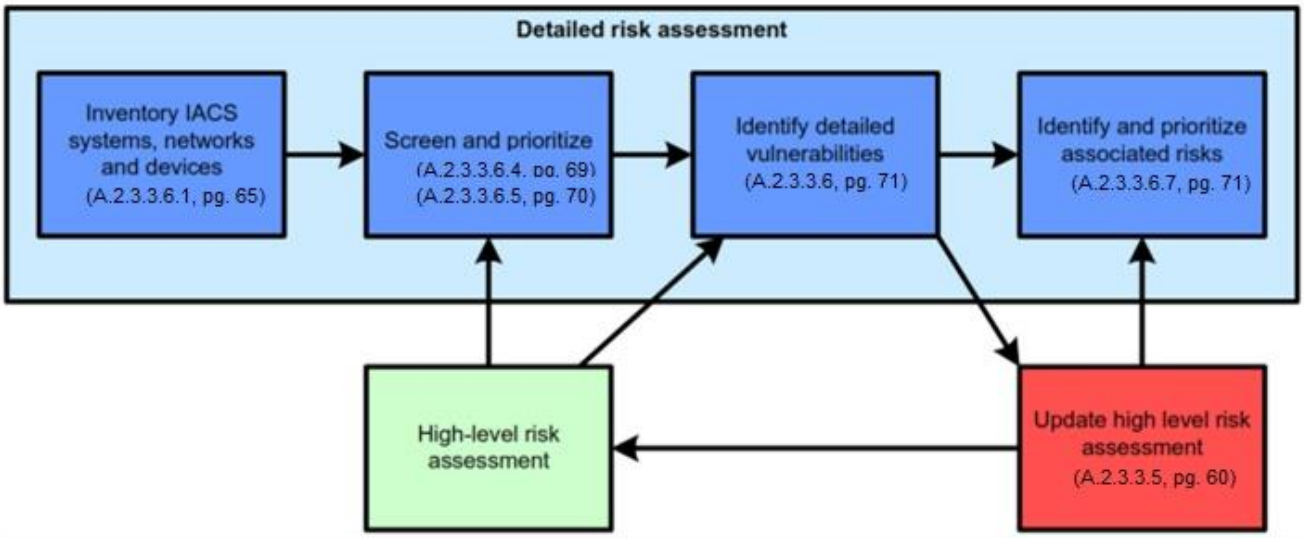
		Consequence category		
		A	B	C
Likelihood	High	High-risk	High-risk	Medium-risk
	Medium	High-risk	Medium-risk	Low-risk
	Low	Medium-risk	Low-risk	Low-risk

ANSI/ISA–62443-2-1, Table A.3, pg 64

Notes:

- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), Annex B.2
- Matrix page 64, Table A.3 Typical risk level matrix
- Someone has to crack the whip to be sure documentation is completed

Detailed Risk Assessment



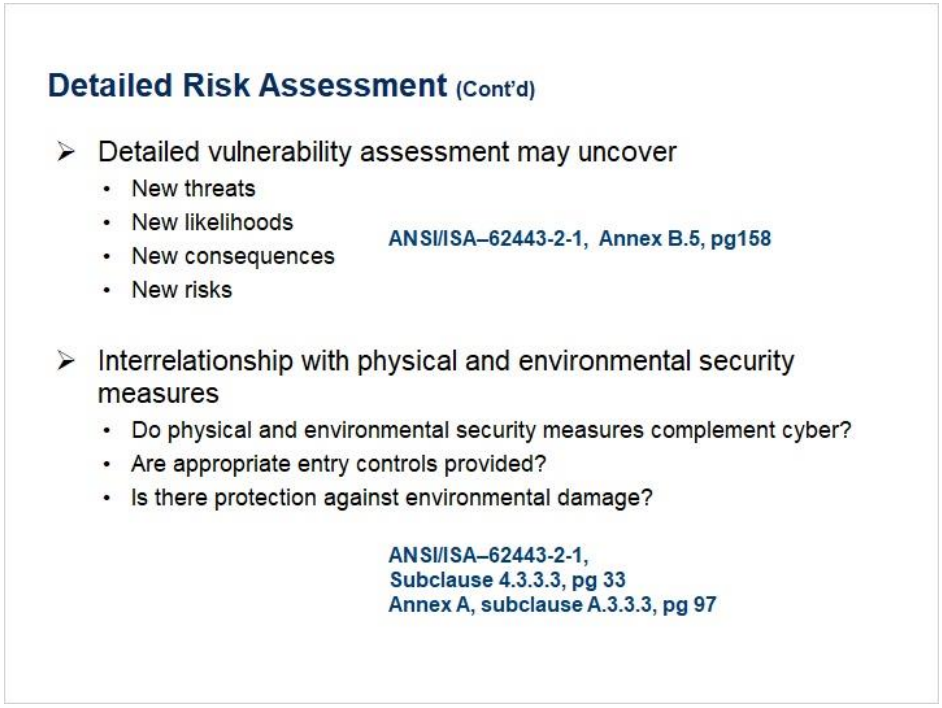
ANSI/ISA–62443-2-1, Fig B.4, pg159

- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), Annex B.2

Detailed Risk Assessment (Cont'd)

- Provide greater detail by first taking an inventory of specific IACS systems, networks, and devices
- Resource or time constraints may not allow detailed examination of all of these assets
  - Use threats, consequences, and types of vulnerabilities identified in the high-level risk assessment to assist in setting priorities to focus on
  - Help desk or maintenance history can help determine focus
- Detailed vulnerabilities guided by the high-level risk assessment vulnerabilities identified
  - Not limited to those high-level vulnerabilities

ANSI/ISA–62443-2-1, Annex B.5, pg158



Notes:

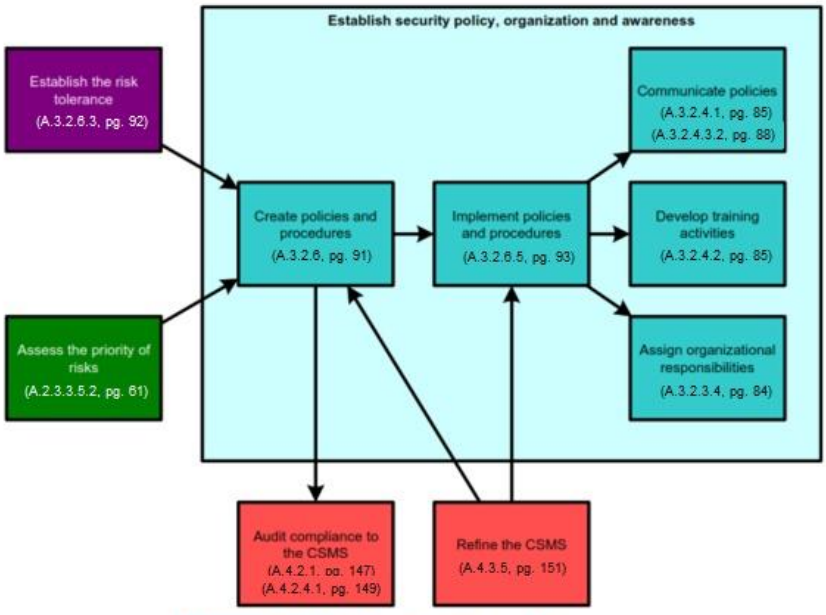
- Noteset Volume II, 62443-2-1, (ANSI/ISA-62443-2-1 (99.02.01)-2009), Annex B.2
- Detailed vulnerability assessment may uncover not only new types of vulnerabilities, but also potentially new threats and associated consequences that had not been identified during the high-level risk assessment - in other words, new risks
- It is easy to get caught into a spiral of identifying vulnerabilities.
- At some point a decision has to be made to move forward and review on next iteration
- Unfortunately, our adversaries do not take a break and are much better at discovering vulnerabilities than we are
- Annex B does not drill down to physical and environmental security
    - Physical security references can be found in this standard and Annex A
    - Subclause 4.3.3.3 pg 33, element: physical and environmental security
    - Annex A, A.3.3.3, pg 97, element physical and environmental security

Detailed Risk Assessment (Cont'd)

- May have to go back and update high-level risk assessment
  - Identified vulnerabilities correctly matched up with specific risk
- Prioritize consistent with method used in high-level risk assessment
- Common pitfall is failure to communicate before, during & after the risk assessment
  - Organizational lack of communication an issue
  - Lack of effective communications
  - Business unit silos

ANSI/ISA–62443-2-1, Annex B.5, pg158

Establish Policy, Organization & Awareness



ANSI/ISA–62443-2-1, Fig B.5, pg160

Establish Policy, Organization & Awareness (Cont'd)

Implementation of policy involves

- Communicating the policy to the organization
- Training personnel in the organization
- Assigning responsibility for adherence to the policy

Policies and procedures can impact any activity in the CSMS

- Countermeasures used drive specific system and maintenance process implementation
- All of these have a cost
- Determining when risk is to be re-assessed

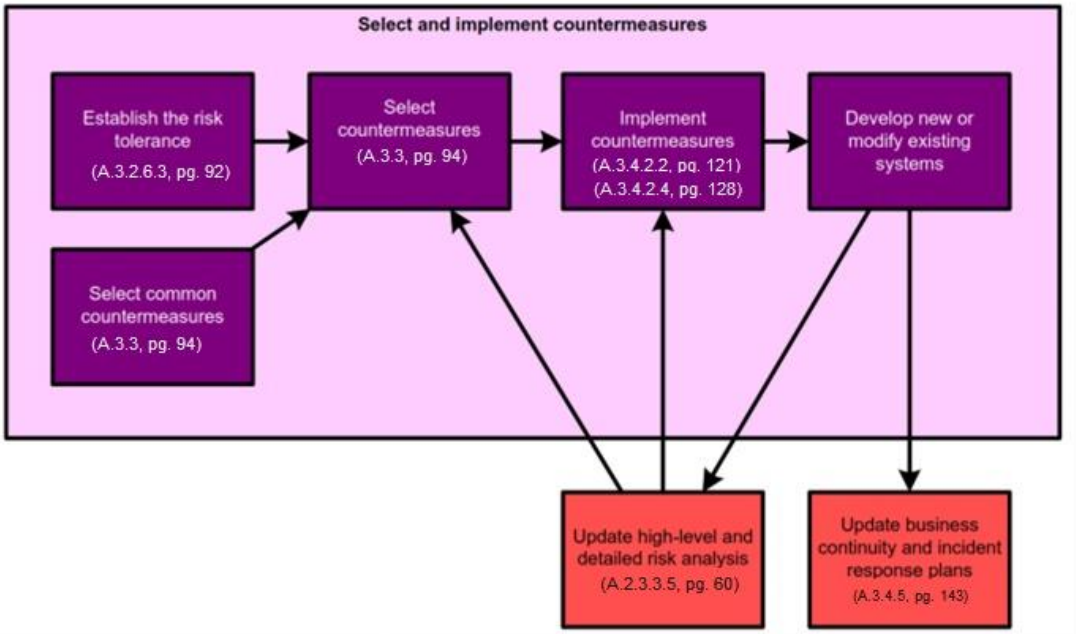
ANSI/ISA–62443-2-1, Annex B.6, pg159-160

Training and Assignment of Responsibilities

- Develop training and assign organization responsibilities
- Over time all organizational responsibilities or training topics related to CSMS should be evaluated
- Part of the iterative process
- Lists may get smaller as program matures

ANSI/ISA–62443-2-1, Fig B.6, pg161-162

Select and Implement Countermeasures



ANSI/ISA–62443-2-1, Fig B.7, pg 162

Select and Implement Countermeasures (Cont'd)

Selection of countermeasures is the technical process of risk management

Driven by:

- Organization's risk tolerance
- Pre-selected common countermeasures
- Results of high-level risk assessment
- Results of detailed risk assessment

ANSI/ISA–62443-2-1, Annex B.7, pg 162

Select and Implement Countermeasures (Cont'd)

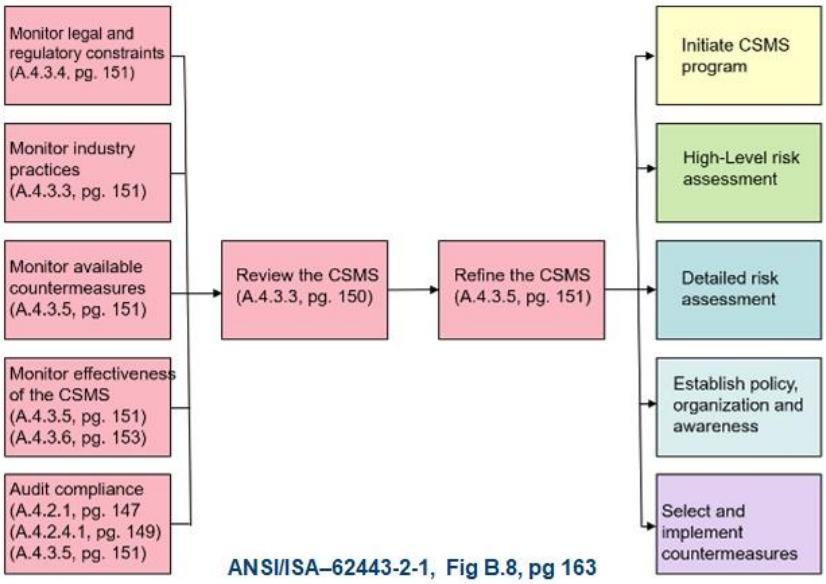
Implementing new or modifying an existing system
- Update high-level risk assessment
- Update detailed risk assessment
- Countermeasures selected based on updated risk info

Development or modification of systems requires
- Update to business continuity plan
- Incident response plan

Common pitfall is that required stakeholders are not invited
- Collaborative processes within organization are immature
- Walls and barriers within the organization exist

ANSI/ISA–62443-2-1, Annex B.7, pg 162

Maintain the CSMS



ANSI/ISA–62443-2-1, Fig B.8, pg 163

Maintain the CSMS (Cont'd)

Maintenance over time requires review and refinement of the CSMS based on review results

Major inputs to this review

- Results from effectiveness measures
- Audits of conformance from internal monitoring

Other inputs to review

- External information about available countermeasures
- Evolving industry practices
- New or changed laws, regulations and mandates

ANSI/ISA–62443-2-1, Annex B.8, pg 162-163

Maintain the CSMS (Cont'd)

Review identifies

- Deficiencies
- Proposes improvements

Use review results to create refinements

Refinements may take the form of

- New countermeasures
- Improvements in countermeasure implementation
- Modify policies and procedures
  - Improve their implementation
  - Review of poor conformance

ANSI/ISA–62443-2-1, Annex B.8, pg 162-163

Maintain the CSMS (Cont'd)

Results may point out the need for improvements in

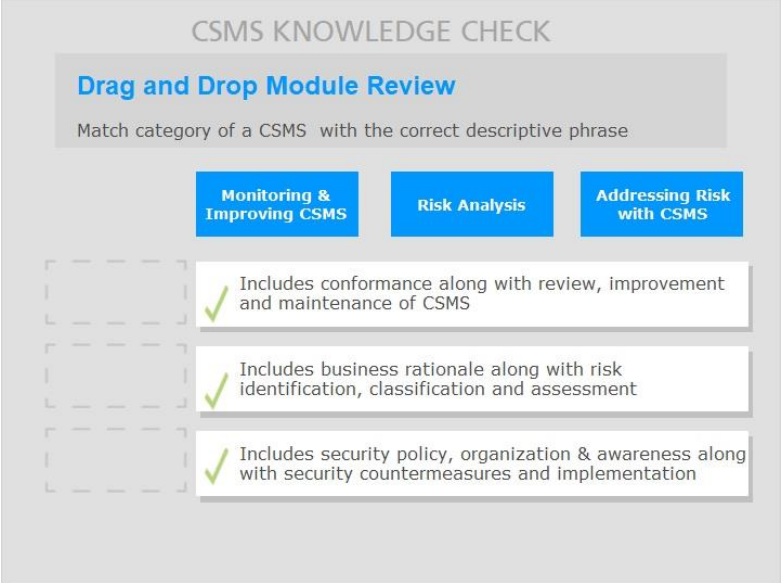
- Training activities
- Organizational responsibilities

Common pitfall is lack of management support thus no resources allocated

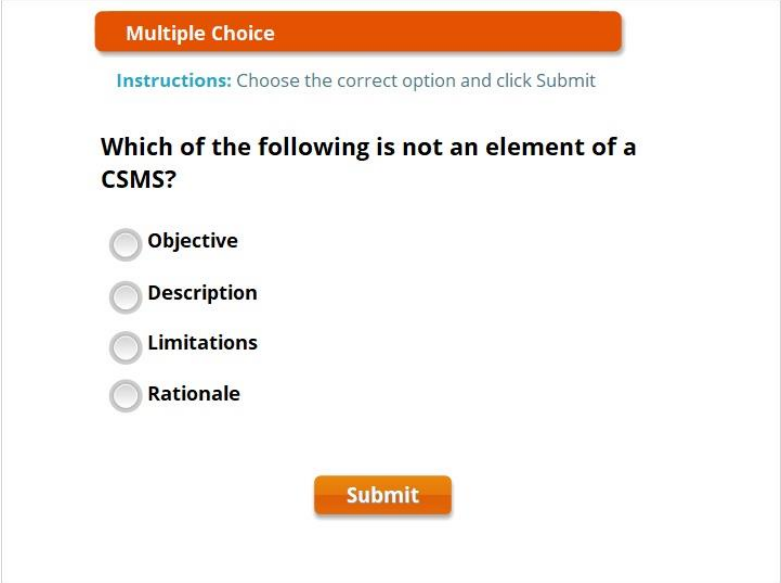
- Cybersecurity fatigue
- Overwhelmed by number of issues

Recap

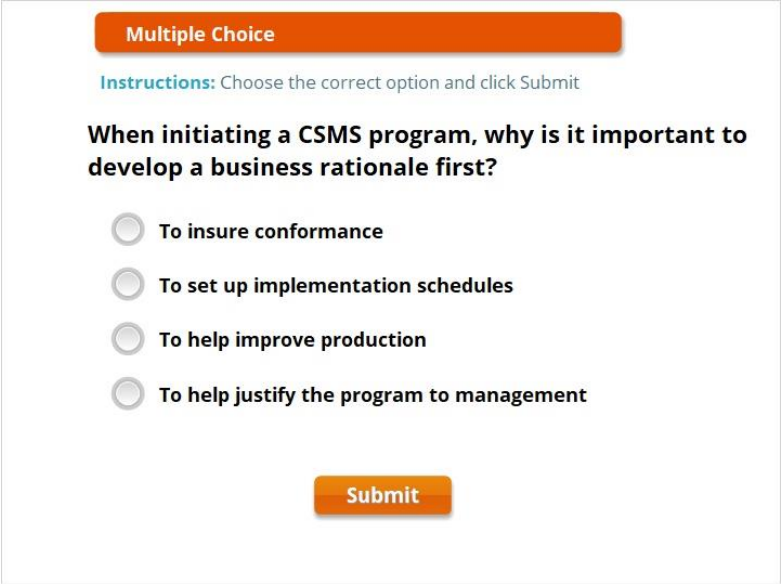
- Policies & Procedures
- Cyber Security Management System (CSMS)
- Process to Develop a CSMS
- CSMS Six Top Level Activities



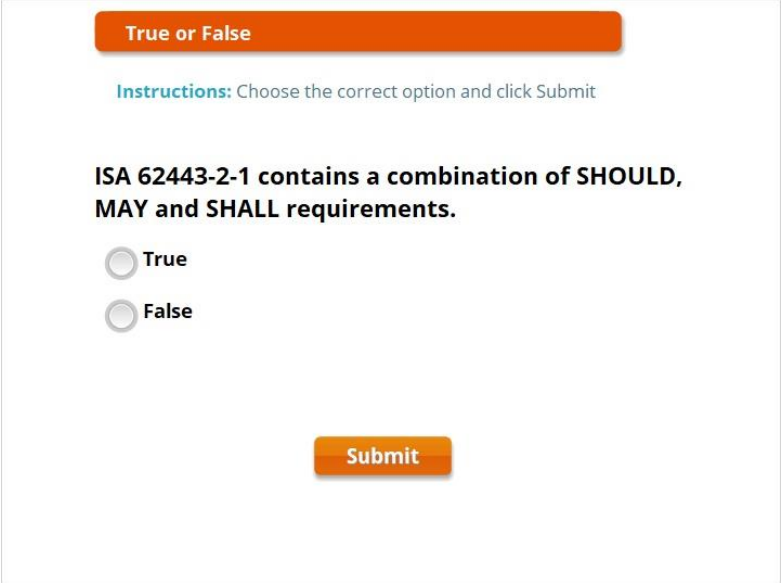
Drag Item	Drop Target
Monitoring & Improving CSMS	Dropzone 1
Risk Analysis	Dropzone 2
Addressing Risk with CSMS	Dropzone 3



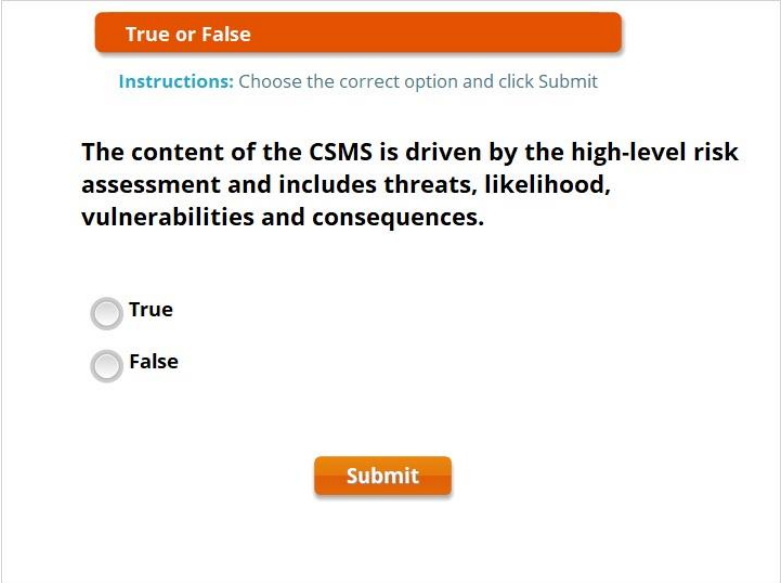
Correct	Choice
X	Radio Button 3



Correct	Choice
X	Radio Button 4



Correct	Choice
X	Radio Button 1



Correct	Choice
X	Radio Button 1

Week 4

Setting the Standard for Automation™

ISA IC329 Module 5

After completing this module you will be able to:

- ✓ Identify and describe the network types typically associated with an IACS.
- ✓ Understand the ISO OSI/Reference model and describe each layer.
- ✓ Identify and discuss differences in IPv4 and IPv6 addressing and ARP protocol.
- ✓ Discuss issues with the OSI model.
- ✓ Discuss the use of network discovery and security auditing tools.

Network Types - WAN

A wide area network (WAN) is a communications system that covers a large geographic area.

Traditionally joined mainframes distributed across the country or world. Now usually joins two or more LANs.

Often uses public networks, such as the telephone system. Can also use private lines, leased lines or satellites.

Three WAN strategies:

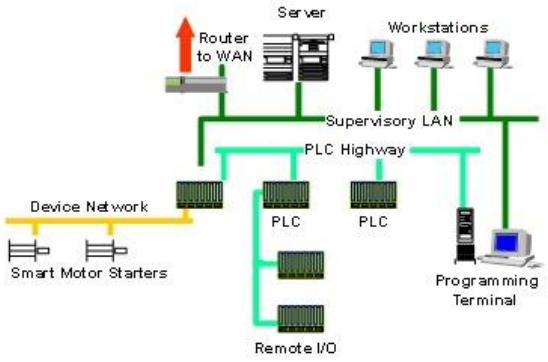
- Enterprise WANs
- Carrier Managed WANs
- Internet

Notes:

- The textbook definition of a WAN is a computer network spanning regions, countries, or even the world. However, in terms of the application of computer networking protocols and concepts, it may be best to view WANs as computer networking technologies used to transmit data over long distances, and between different LANs, MANs and other localized computer networking architectures

Network Types - LAN

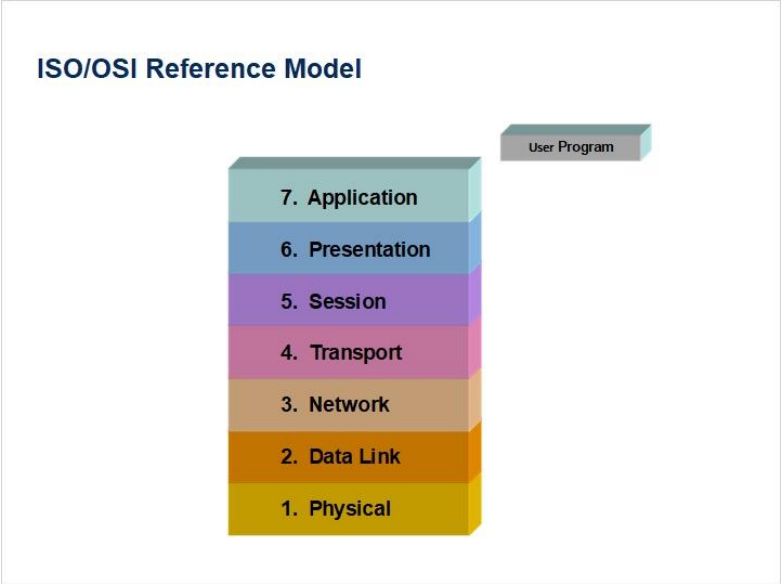
- A local area network (LAN) is a communications system that covers a limited distance (usually under 10 km), generally within a single facility.
- LAN technologies are used in the factory under many names:
  - Supervisory Networks
  - DCS Highways
  - PLC Highways`
  - Fieldbuses
  - Device Networks



Notes:

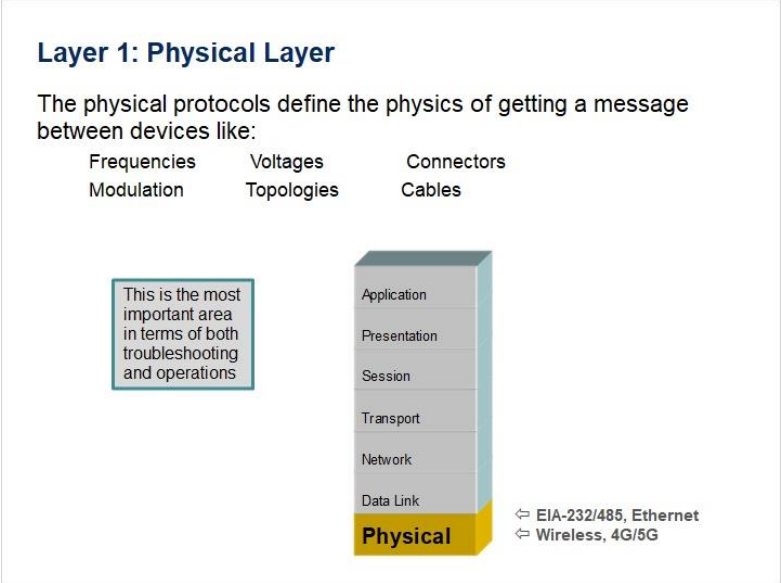
- A **local area network (LAN)** is a computer network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building using network media.[1] The defining characteristics of LANs, in contrast to wide area networks (WANs), include their usually higher data-transfer rates, smaller geographic area, and lack of a need for leased telecommunication lines
- Generally if you own it then it is probably a LAN

2.9 ISO/OSI Reference Model



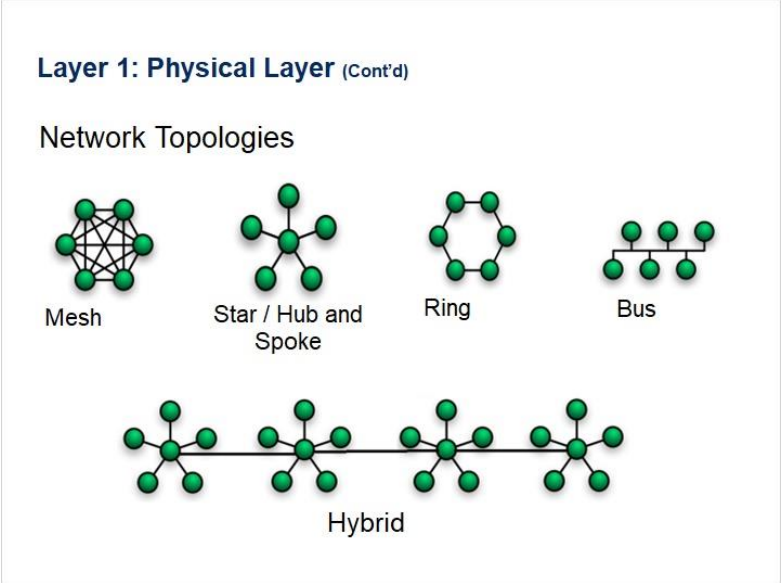
Notes:

- The OSI, or Open System Interconnection, model defines a networking framework for implementing protocols in seven layers
- Also referred to as “the stack”
- A seven-layer cake
- It is a conceptual framework to better understand complex communications
- Data payload is passed from one layer to the next,
    - starting at the application layer in one station,
    - proceeding to the bottom layer,
    - over the channel to the next station and back up the stack



Notes:

- Physical layer protocols are concerned with the physics of getting a message from one device to another:
    - Electrical characteristics such as modulation frequencies & voltage levels.
    - Mechanical characteristics that specify the physical connector.
    - Standards for cables, connectors, wiring topologies and or signaling techniques.
- From an industrial maintenance point of view, this layer is the most important area in terms of troubleshooting, accounting for 80% of all network problems
- Some very well-known standards are Physical layer standards:
- **EIA-232 aka RS232** - The original modem to terminal wiring standard. Used throughout industry for interconnecting devices from different vendors, such as PLC to DCS links.
- **EIA-485** aka RS485 - The electrical specifications of EIA-422 modified so that a single pair of wires can be used for both transmit and receive. Now used as the physical layer for many vendors' remote I/O or device buses (e.g. Profibus).
- **Ethernet (IEEE 802.3**) - Physical and Data Link layer standard
    - MAC (Layer 2) addressing, duplexing, differential services, and flow control attributes,
    - Physical (Layer 1) definitions, with media, clocking, and speed attributes

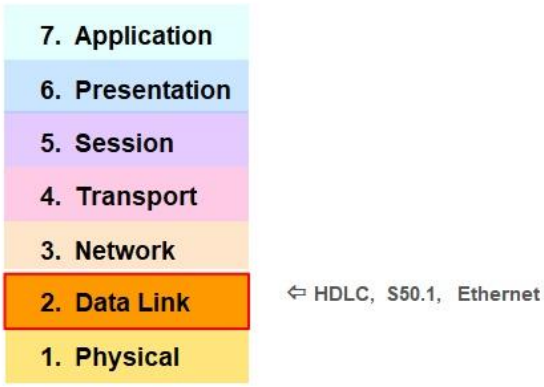


Notes:

- The physical layer defines the means of transmitting raw bits rather than logical data packets over a physical link connecting network nodes. The bit stream may be grouped into code words or symbols and converted to a physical signal that is transmitted over a hardware transmission medium. The physical layer provides an electrical, mechanical, and procedural interface to the transmission medium. The shapes and properties of the electrical connectors, the frequencies to broadcast on, the modulation scheme to use and similar low-level parameters, are specified here
- **Star networks** are one of the most common computer network topologies. In its simplest form, a star network consists of one central switch, hub or computer, which acts as a conduit to transmit messages. This consists of a central node, to which all other nodes are connected; this central node provides a common connection point for all nodes through a hub. In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch. The switch is the server and the peripherals are the clients.
- **Mesh Topology** is a type of networking where each node must not only capture and disseminate its own data, but also serve as a *relay* for other nodes, that is, it must collaborate to propagate the data in the network.
- There are 2 forms of Mesh topology: Partially connected
- **ring network** is a network topology in which each node connects to exactly two other nodes, forming a single continuous pathway for signals through each node - a ring. Data travels from node to node, with each node along the way handling every packet.
- **Bus Topology** connects all nodes to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted

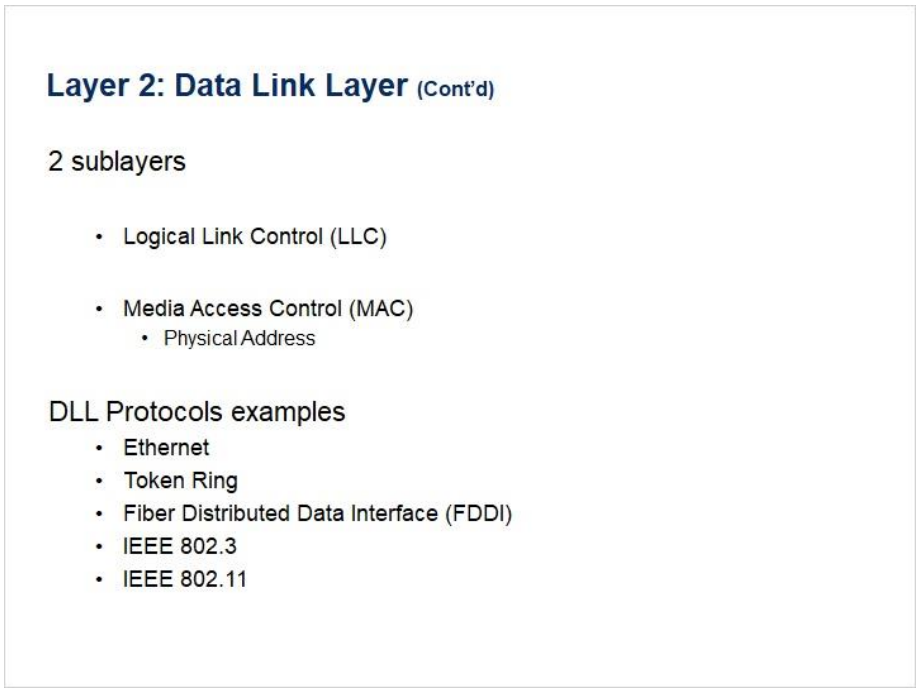
Layer 2: Data Link Layer

- Provides the rules for framing, converting electrical signals to data, error checking, physical addressing and media access control (which station can talk at any given time on the network)
- Every communications network needs some data link protocols



Notes:

- Layer two is extremely important to data communications because this is where the binary digital 1s and 0s are organized into transmission entities (blocks, packets, frames).
- Thus protocols at this layer will define how to mark the start and end of a transmitted block or frame.
- Physical node addressing and error detection is done by protocols at this layer.
- On any system where devices share the media (such as Ethernet LANs), the protocols at this layer look after Media Access Control. Master/Slave is a simple example of a MAC protocol and is used by Modbus RTU.
- Some early Data Link protocols are **Bi-sync** and **RTU** (of MODBUS Fame).
- More sophisticated examples of Data Link protocols are **HDLC** and **Ethernet** and the Data Link layer of **S50.1** (Foundation Fieldbus). Again, notice that Ethernet spans two layers.
- **Definitions:**
    - **HDLC** (High-Level Data Link Control) - A bit-oriented framing system used by Modbus+, smart modems and many, many other systems.
    - **Bi-Sync** (Binary Synchronous) - An old IBM character-based block synchronizing method.



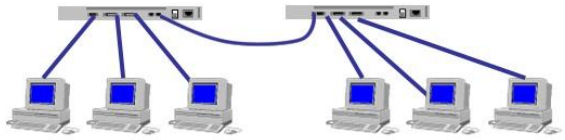
Notes:

- Layer two is extremely important to data communications because this is where the binary digital 1s and 0s are organized into transmission entities (blocks, packets, frames). Thus protocols at this layer will define how to mark the start and end of a transmitted block or frame. Physical node addressing and error detection is done by protocols at this layer. **The data link layer is concerned with local delivery of frames between devices on the same LAN.** Data-link frames, as these protocol data units are called, do not cross the boundaries of a local network. Inter-network routing and global addressing are higher layer functions, allowing data-link protocols to focus on local delivery, addressing, and media arbitration. In this way, the data link layer is analogous to a neighborhood traffic cop; it endeavors to arbitrate between parties contending for access to a medium.
- Data link layer connects hosts within the same network
- **media access control (MAC)** sub layer function manages the interaction of devices with a shared medium.
- Above this MAC sub layer is the media-independent IEEE 802.2 **Logical Link Control (LLC)** sub layer, which deals with addressing and multiplexing on multi-access media.
- **IEEE 802.3 Ethernet** is the dominant wired LAN protocol and **IEEE 802.11** the dominant wireless LAN protocol

2.14 Layer 2 Switches

Layer 2 Switches

- Layer 2 Switches work at physical and data-link layer within a single LAN
- More advanced than a hub because a switch will only send a message to the device that needs or requests it
- MAC address used to decide where to forward frame



Notes:

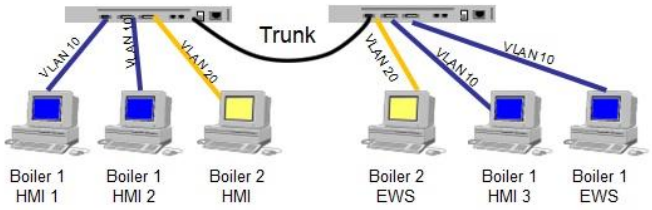
- A bridge is used to connect separate but related networks together or divide a larger network into two or more small networks. Working at the second protocol layer (the Data Link layer) bridges open and check packets that they receive. Most can learn addresses of the devices on each port, forwarding only the necessary traffic through.
- Layer 3 Switches described in layer 3 section

Managed versus Unmanaged Switches

UNMANAGED	MANAGED
Not configurable Plug-and-play	Configurable local/remote
Home/small business	Supports advanced functions

Virtual Local Area Network (VLAN)

- Partition a Layer 2 network (LAN) into multiple distinct segments (a.k.a. broadcast domains)
- Enables grouping of hosts with common requirements regardless of their physical location
- VLAN protocols (e.g., IEEE 802.1Q) tag frames with VLAN information
- Can work hand in hand with QoS to prioritize time sensitive traffic



Notes:

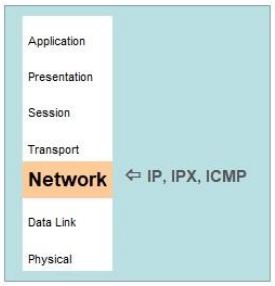
- QoS = Quality of Service
  - Sports channel gets priority ☺
  - Online gaming

Layer 3: Network Layer

The protocols at the Network layer deal with routing of messages through a complex network

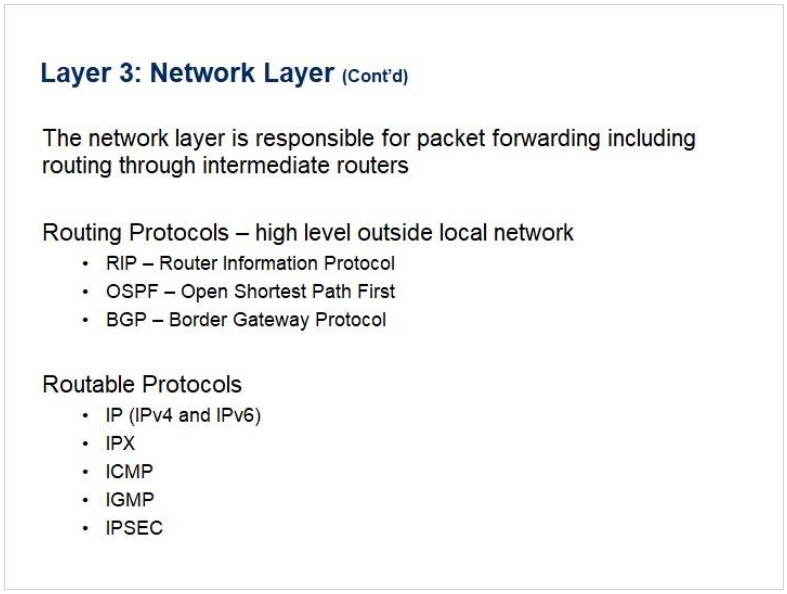
For example, finding the best route through a network

IP of TCP/IP fame is one example of a network layer protocol



Notes:

- Some definitions:
  - **IP** - Internet Protocol - the routing protocol used on the Internet to find a route for a packet from say, Boston to RTP.
  - **IPX** - Internetwork Packet Exchange (An industrial example is Koyo, who used to employ IPX for PLC to I/O block communications)
  - **Internet Control Message Protocol** (**ICMP**) eg PING Layer 3 protocol https://tools.ietf.org/html/rfc792 (retrieved 13 Dec 2016)



Notes:

- The network layer provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network (in contrast to the data link layer which connects hosts within the same network), while maintaining the quality of service requested by the transport layer. The network layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors.
- **Routers operate at this layer**, sending data throughout the extended network and making the Internet possible. This is a logical addressing scheme - values are chosen by the network engineer. The addressing scheme is not hierarchical.
- The network layer may be divided into three sub layers:
    - Sub-network access - that considers protocols that deal with the interface to networks, such as X.25;
    - Sub-network-dependent convergence - when it is necessary to bring the level of a transit network up to the level of networks on either side
    - Sub-network-independent convergence - handles transfer across multiple networks.
- **Border Gateway Protocol** (**BGP**)
- **Routing Information Protocol** (**RIP**)
- **Open Shortest Path First** (**OSPF**)
- **Internet Control Message Protocol** (**ICMP**) Layer 3 protocol https://tools.ietf.org/html/rfc792 (retrieved 13 Dec 2016)
- **Internet Group Management Protocol** (**IGMP**)
- **Internet Protocol Security** (**IPsec**)
- **Internetwork Packet Exchange** (**IPX**)

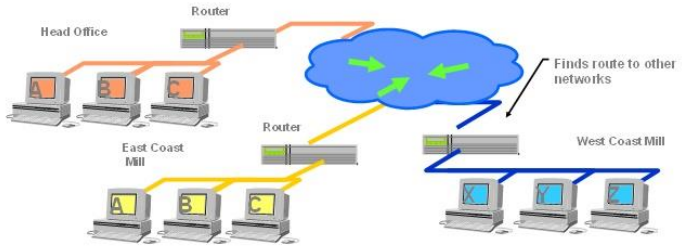
Layer 3 Networking Equipment

Routers

Layer 3 Switches

Routers

- Router is a Layer 3 device that connects a WAN to a LAN
- Divides big network into logical sub-networks
- Routers need to be configured with an IP routing table (static or dynamic)

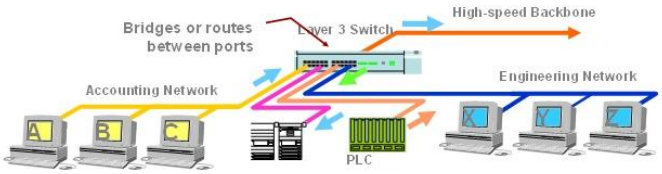


Notes:

- Operating at the third or Network layer of the OSI model, routers interconnect complex networks, such as the Internet or a corporate wide area network (WAN). Communicating with other routers, they select the best possible route for a message, based on criteria such as availability, cost, loading and speed.
- Routers are intelligent devices used to divide networks logically rather than physically. For example, an IP router can divide a network into various subnets so that only traffic destined for particular IP addresses can pass between segments.
- ISA99 Master Glossary definiton:
    - Gateway between two networks at OSI layer 3 and that relays and directs data packets through that inter-network
    - Note: The most common form of router passes Internet Protocol (IP) packets.

Layer 3 Switches

- Layer 3 Switches are switches with routing capabilities **but no WAN connection**
- Will act like a switch when it is connecting devices on the same LAN (subnet)
- Will act like a router to route traffic **between different subnets**

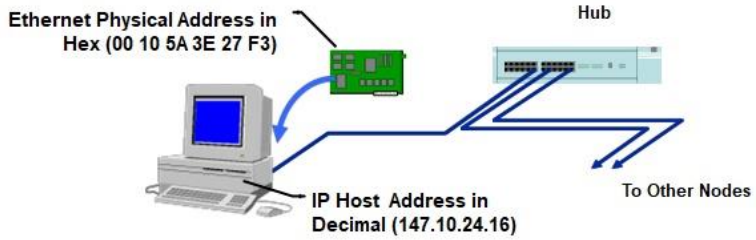


Notes:

- A switch is basically a multi-port bridge (a layer-two switch) or multi-port router (a layer-three switch) with a very high-speed backplane.
- Each port connects to an independent network and the high-speed backplane transfers the messages between ports.
- Switching technology has emerged as the evolutionary heir to bridging in many networks. Where bridging technology was once used, switches now dominate, due in part to their superior performance, lower per-port cost, and greater flexibility. But at their core, switches are still just fancy bridges or routers.

IPv4 Addressing

- Every device in a TCP/IP network needs a unique IP address
- IPv4 uses a 32 bit address written in the quad-dotted form:
  147.10.24.16
- Each number (0-255) is the decimal coding for 8 bits (octet)
- Allows close to 4.3 billion addresses (4.3×10^9)

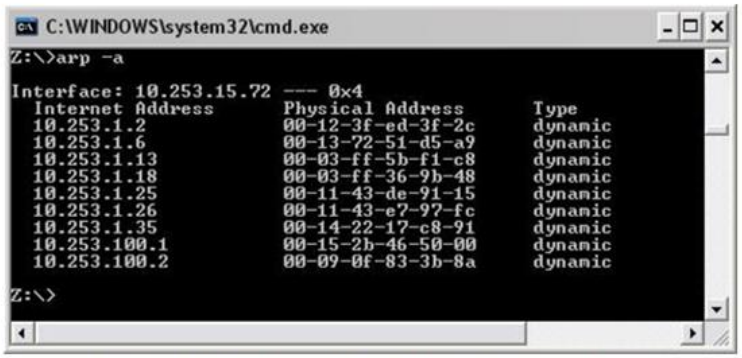


Notes:

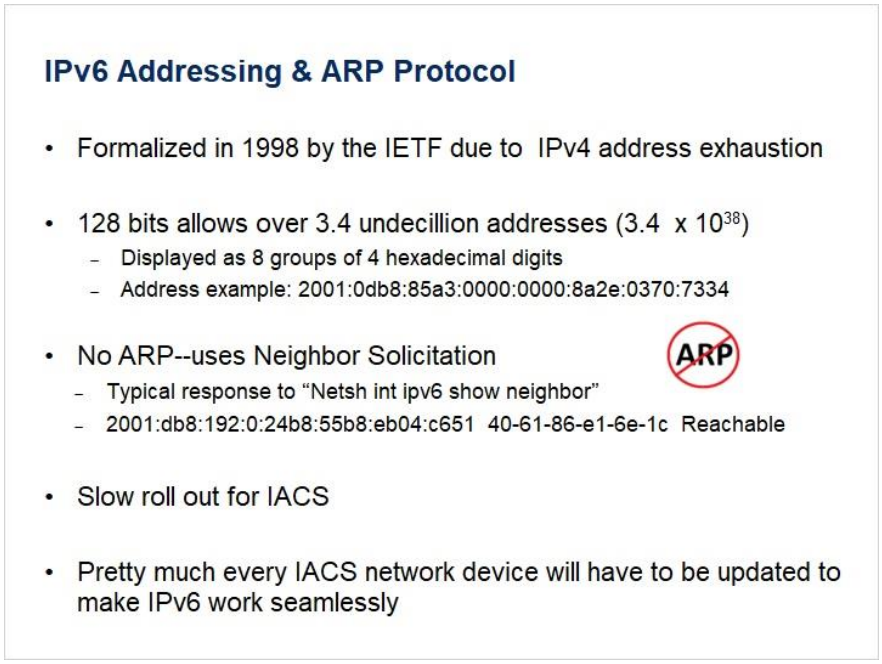
- This address is different from the Ethernet physical address (MAC)
- IPv4 is 32 bits (2^{32}) and allows close to 4.3 billion addresses.
  - The way they are allocated is very inefficient.
  - 4,294,967,296 addresses; if they could all be assigned

ARP Protocol

- Address Resolution Protocol (IPv4)
- Resolve Network Layer (3) addresses to Data Link Layer MAC or Physical Addresses (2)
- Ethernet networks converts an IP address to a MAC address

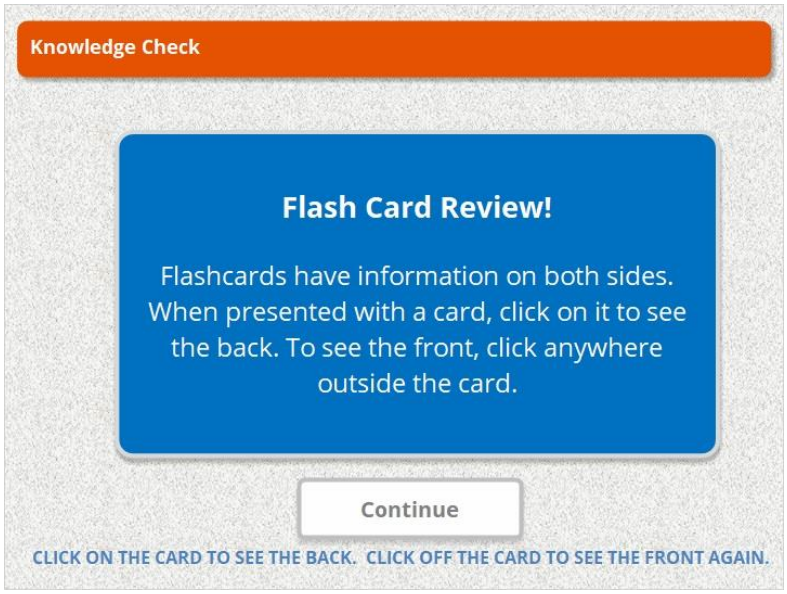


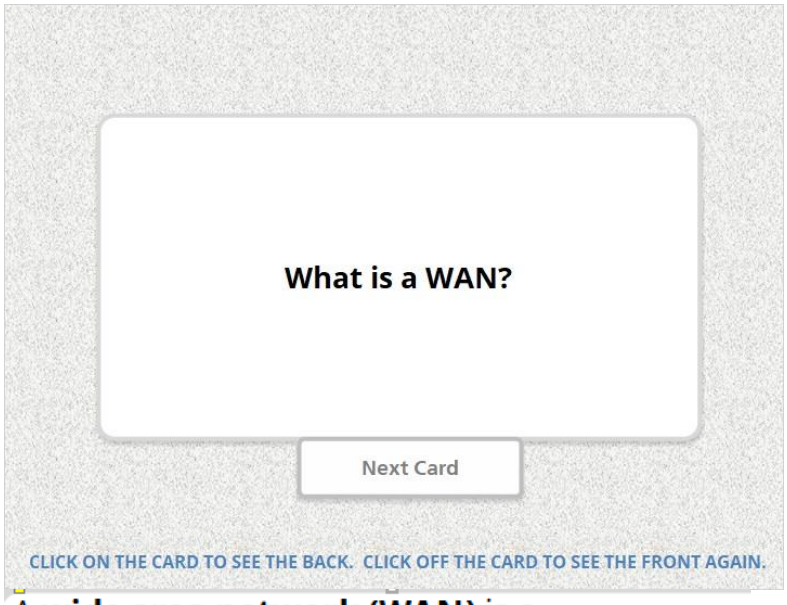
Typical ARP Table (ARP Cache) in a Windows PC



Notes:

- Internet Engineering Task Force (IETF)
- Recommend that IPv6 topic deep dive is for the students to pursue on their own
    - TS06 or TS12 may cover more on IPv6
- IPv6 is 128 bits (2^{128}) and allows over 3.4 undecillion addresses.
    - 340,282,366,920,938,463,374,607,431,768,211,456 addresses if all could be assigned
- Comparison of addresses
    - 4.3 billion addresses (4.3×10^9) IPv4
    - 3.4 undecillion addresses (3.4×10^{38}) IPv6
    - Currently dual stack IPv4 and IPv6 environment
- No ARP and use of Neighbor Solicitation is a course in itself
    - Example W10 Pro command to show neighbors: "Netsh int ipv6 show neigh"
- IPv6 Internet Service Providers (ISP) products and services launching since 6 June 2012
    - 20% of top websites are reachable over IPv6
    - http://www.worldipv6launch.org/measurements/ (retrieved 9 Dec 2016)


Knowledge Check
Flash Card Review!
Flashcards have information on both sides. When presented with a card, click on it to see the back. To see the front, click anywhere outside the card.
Continue
CLICK ON THE CARD TO SEE THE BACK. CLICK OFF THE CARD TO SEE THE FRONT AGAIN.



A **wide area network (WAN)** is a communications system that covers a large geographic area.

WANs are computer networking technologies used to transmit data over long distances, and between different LANs, MANs and other localized computer networking architectures.

A **local area network (LAN)** is a computer network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building using network media.

The defining characteristics of LANs, in contrast to WANs, include their usually higher data-transfer rates, smaller geographic area, and lack of a need for leased telecommunication lines

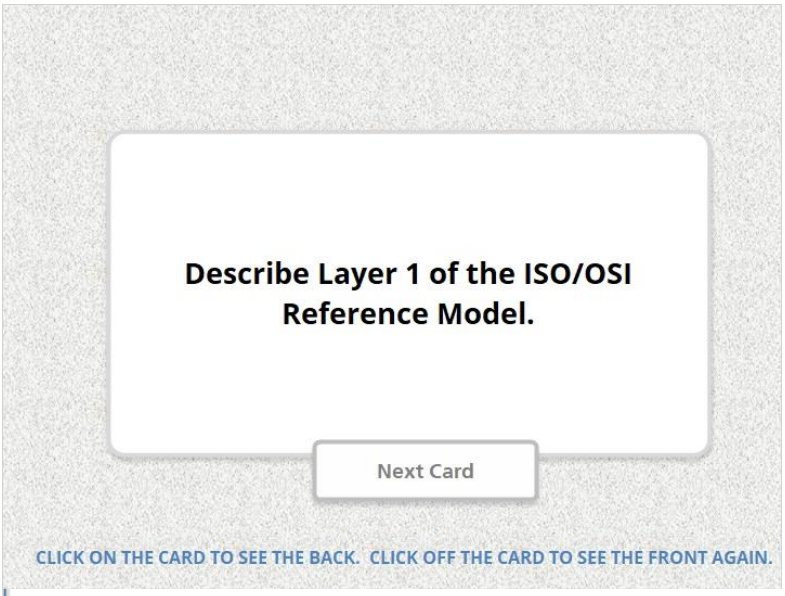
Describe Layer 3 of the ISO/OSI Reference Model.

Next Card

CLICK ON THE CARD TO SEE THE BACK. CLICK OFF THE CARD TO SEE THE FRONT AGAIN.

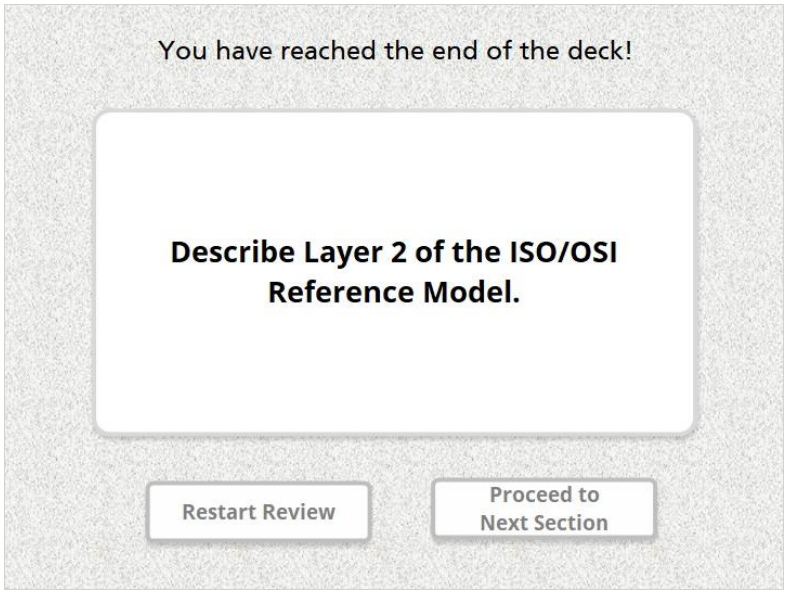
Layer 3: Network Layer

- The protocols at the Network layer deal with routing of messages through a complex network (finding the best route through a network.)
- IP of TCP/IP fame is one example of a network layer protocol
- Routing Protocols – high level outside local network
  - RIP – Router Information Protocol
  - OSPF – Open Shortest Path First
  - BGP – Border Gateway Protocol
- Routable Protocols
  - IP (IPv4 and IPv6)
  - IPX
  - ICMP
- IGMP
- IPSEC



Physical layer protocols are concerned with the physics of getting a message from one device to another:

- Electrical characteristics such as modulation frequencies & voltage levels.
- Mechanical characteristics that specify the physical connector.
- Standards for cables, connectors, wiring topologies and/or signaling techniques.
- EIA-232/485, Ethernet



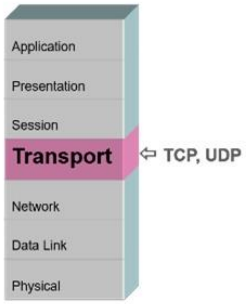
Layer 2: Data Link Layer

- Provides the rules for framing, converting electrical signals to data, error checking, physical addressing and media access control (which station can talk at any given time on the network.)
- 2 sublayers
  - Logical Link Control (LLC)
  - Media Access Control (MAC)
  - Physical Address
- DLL Protocols examples
  - Ethernet
  - Token Ring
  - Fiber Distributed Data Interface (FDDI)
  - IEEE 802.3
  - IEEE 802.11

Module 5 Part 2

Layer 4: Transport Layer

- Provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control
- It ensures complete data transfer
- Numbers packets to keep them in order
- TCP of TCP/IP fame is one example of a transport protocol



Notes:

- The transport layer makes the end nodes appear as if they are directly connected. It tries to hide all the intermediate devices and conversions.
- Example of a Transport function is to number the packets as they are sent out. If the packets get out of order as they travel across a large network, the receivers transport protocol will sort them out again.
- Some definitions:
    - **TCP/IP** - Transport Control Protocol/Internet Protocol
    - **SPX** - Sequential Packet Exchange-Novell NetWare Operating System
        - Novell ceased to exist in 2010
        - IPX/SPX lost out to TCP/IP
            - Could be found in legacy system, won't run on internet
    - **UDP -** User Datagram Protocol
    - **NetBeui** - A transport layer protocol used in small and simple Microsoft office networks.

Layer 4: Transport Layer (Cont'd)

Transport Layer Functions

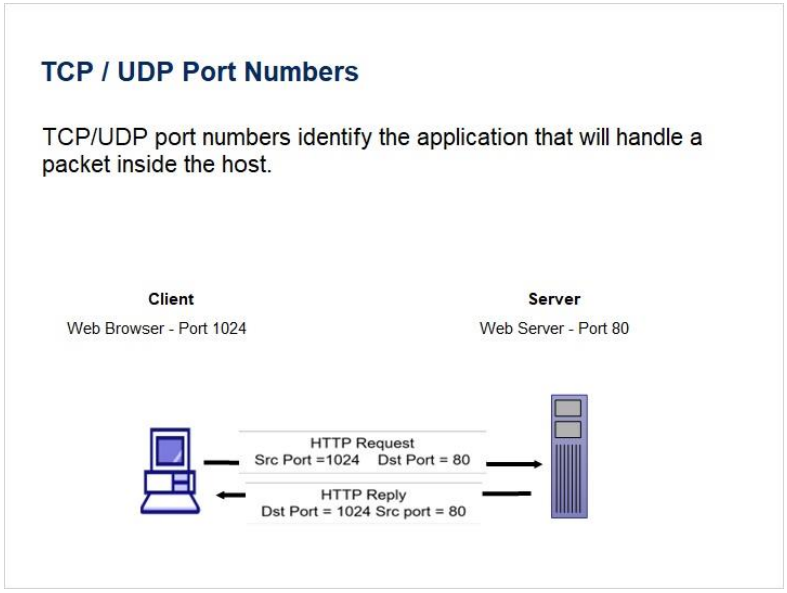
- Flow Control
- Multiplexing
- Virtual Circuit Management
- Error Checking and Recovery

Transport Layer Protocols

Protocol	Name	Use
TCP	Transmission Control Protocol	Connection based
UDP	User Datagram Protocol	Send and forget
DCCP	Datagram Congestion Control Protocol	Connection setup & teardown
SCTP	Stream Control Transmission Protocol	UDP with TCP delivery assurance
RSVP	Resource Reservation Protocol	A control protocol

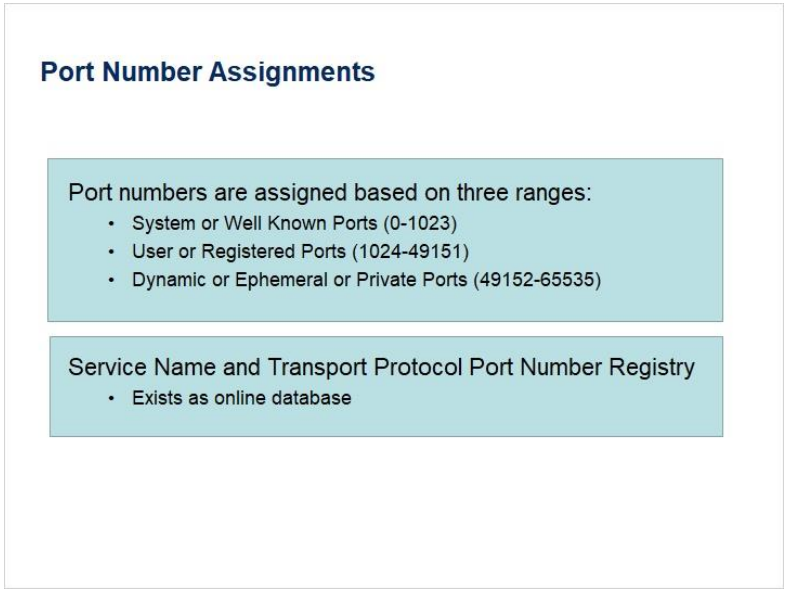
Notes:

- The transport layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The transport layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control. Some protocols are state- and connection-oriented. This means that the transport layer can keep track of the segments and retransmit those that fail. The transport layer also provides the acknowledgement of the successful data transmission and sends the next data if no errors occurred.



Notes:

- Describe how communications on UDP and TCP occur over ports
- Use the graphic to explain a Web browser connection
- Explain Well Known Port Numbers for services
- Explain dynamical port assignment for client
- Consider demonstrating a connection. After making the connection, you can use netstat to show connection information



Notes:

- The three ranges are described in RFC 6335, pages 10 and 19
- Ephemeral means temporary or short-lived
    - Operating systems (OS) use different ephemeral port ranges
    - Many Linux versions use port range 32768-61000
    - Windows versions (until XP) use 1025-5000, by default
    - Vista, Windows 7 and Server 2008, use the Internet Assigned Number Authority (IANA) suggested range of 49152-65535
- RFC 1700 originally defined port numbers, now obsolete-DO NOT USE
- RFC 1700 port list has been replaced by an online database Service Name and Transport Protocol Port Number Registry found at:
    - http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml (retrieved 9 Sep 2017)
    - Available formats csv, xml, html, plain text can be downloaded

Layer 5: Session Layer

- Session is a persistent logical linking of two software application processes
- Provides the mechanism for opening, closing and managing a session between end-user application processes
  - Associated with TCP/UDP port numbers
- Each OS handles session data differently
- Example protocols:
  - Layer 2 Tunnelling Protocol (L2TP)
  - Point-to-Point Tunnelling Protocol (PPTP)
  - Remote Procedure Calls (RPC)

Notes:

- The session layer controls the dialogues (connections) between computers.
- Session is a persistent logical linking of two software application processes
  - It is application centric where L4 Transport is host centric.
- It establishes, manages and terminates the connections between the local and remote application.
- It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures.
- The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session checkpointing and recovery, which is not usually used in the Internet Protocol Suite.
- The session layer is commonly implemented explicitly in application environments that use remote procedure calls.
- On this level, Inter-Process communication (IPC) happen (SIGHUP, SIGKILL, End Process, etc.)
- Sockets interface lies conceptually at layer five and is used by TCP/IP application programmers to create sessions between software programs over the Internet on the UNIX operating system.
- Windows Sockets similarly lets programmers create Windows software that is Internet-capable and able to interact easily with other software that uses that interface. (Strictly speaking, Sockets is not a protocol, but rather a programming method.)
- Every PLC, DCS has its own OS

Layer 6: Presentation Layer

- Presentation layer functions are generally handled in the Application layer (FTP, SMTP, Telnet, etc.)
- Deals with data format conversion and possibly with encryption and security
  - Associated with Secure Sockets Layer (SSL)
- Responsible for the delivery and formatting of information to the application layer for further processing or display (if used)

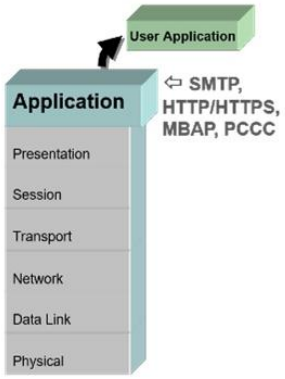
Notes:

Presentation:

- Note that this is an ambiguously defined layer and has been criticized formally many times and is debatable as a separate layer.
- Most of the time its functions are carried out by protocols at other layers.

Layer 7: Application Layer

- Interacts with software applications that implement a communicating component
- Protocols specific to network applications such as email, file transfer and reading data registers in a PLC
- Does not include user applications like word processing or operating systems like Windows-XP or Windows 7

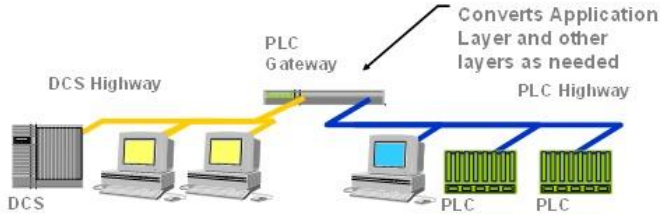


Notes:

- Stress that Application Layer protocols specify the rules to achieve specific tasks over a network. For example, **MBAP** (Modbus Application Protocol) or **PCCC** (Allen-Bradley) each define the command structure to read a set of registers from a PLC. Similarly, **SMTP** (Simple Mail Transfer Management Protocol) provides a standard method of sending emails across an network.
- The user software applications et "Office, Outlook, Excel, Games" are above this layer
- The application layer protocols are in a much more confused state of affairs, especially in the industrial market. There are many more proprietary protocols and only a few widely accepted standards.
- While TCP and IP are two mid-level protocols, it is traditionally grouped with some upper level protocols that are very useful:
    - **FTP** - File Transfer Protocol allows you to transfer files, regardless of type of computer system.
    - **SMTP** - Simple Mail Transfer Management Protocol provides a standard method of sending emails across an network
    - **Telnet** - A protocol that allows your desktop computer to communicate over a network as if it were a dumb terminal attached to a main frame.
    - **HTTP** - Hyper Text Transfer Protocol allows your web browser to read the layout of a web page so it can display it on your computer.
- All E-Mail Use SMTP,POP-3, IMAP4: G-mail, Outlook, Yahoo, AOL
- All Browsers Use HTTP: IE, Google, Chrome, Firefox, Mozilla

Layer 7 Gateways

- Gateways are a layer-seven device
  - This is not the “default gateway” network interface card setting
- Gateways connect two completely differing network systems (e.g., DCS to PLC)
- Also used to provide application layer conversions (e.g. between two different email systems)



Notes:

- Gateways provide support for all seven layers of protocol and thus can connect completely different systems.
- For example, gateways are often used to connect a DCS highway to a PLC highway or a Novell LAN to IBM Mainframe.
- Because they have to interpret all seven layers of protocols most gateways are relatively slow and expensive.
- Can be a specifically designed machine or two different adapter cards in a PC with a program to interface the two.
- Do not confuse this gateway with the “default gateway” network card setting

Problems with the OSI Model

- OSI layer specifications are functional only
  - What to do is defined
  - How to do it is not

- Two protocol families that are "ISO compatible" won't necessarily communicate
- It is too complex for many applications (such as industrial fieldbuses) so layers are skipped, typically L5 & L6
  - PLC, DCS have unique OS, memory management, scan management
- But it does give us a good starting point to organize all those protocols...

Notes:

- FYI: Tanenbaum in the classic textbook, *Computer Networks,* describes some of the serious technical problems with the OSI/RM, particularly with the definition of communications between layers. However, this is beyond the level of this course.
- He does point out that the choice of seven layers was rather arbitrary and some countries wanted a five-layer model.
- In addition, some layers are overloaded (e.g. Data Link) and some are poorly defined (e.g. Session).
- But for a committee effort it wasn't too bad :-)
- Stress that the model has given us a protocol filing system that helps us understand how all the network technology and terminology inter-relates.

Intro Network Discovery and Security Auditing Tools

Many free and open source tools such as

- Nmap
- SuperScan

Tools useful for tasks

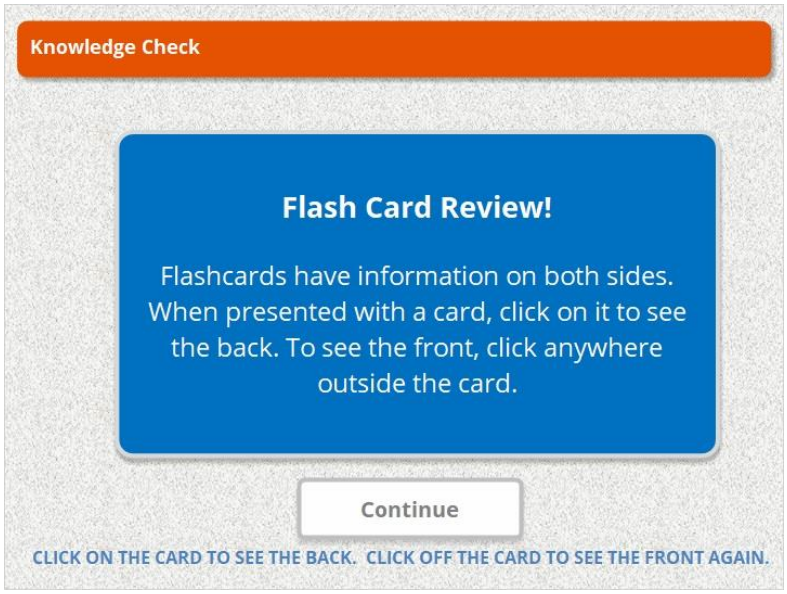
- Network inventory
- Managing service upgrade schedules
- Monitoring host or service uptime

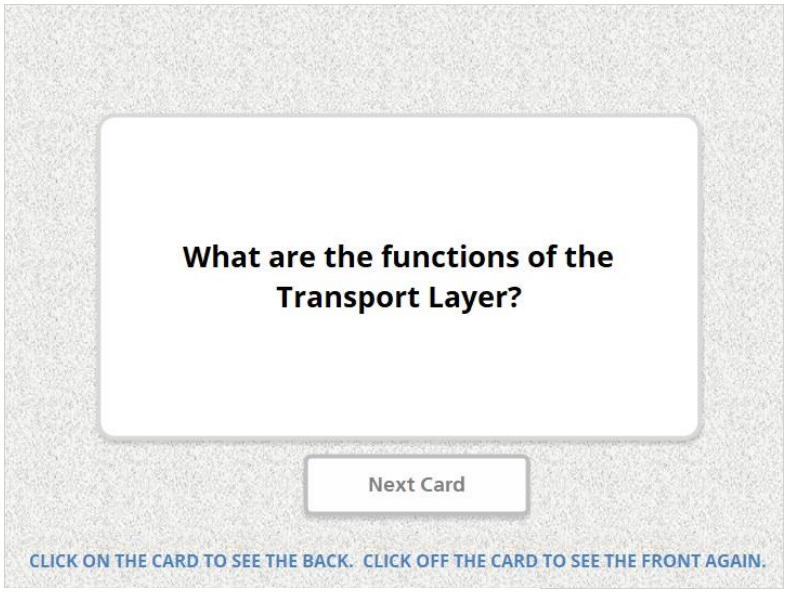
Tools also useful by unauthorized personnel

- Scan and "fingerprint" network
- Services (application name and version)
- Operating systems (and OS versions)
- Type of packet filters/firewalls are in use

Notes:

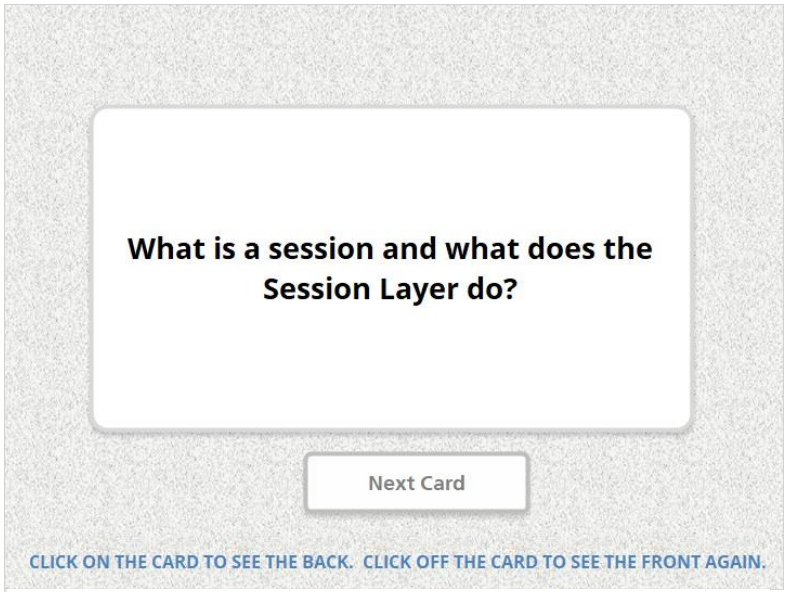
- Tools are a double edged sword
- Many systems and network administrators find these tools useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.
- However, these tools may also be used by unauthorized personnel to scan and "fingerprint" a network.
- These tools use raw IP packets to determine what hosts are available on the network,
- what services (application name and version) those hosts are offering,
- what operating systems (and OS versions) they are running,
- what type of packet filters/firewalls are in use,
- and dozens of other characteristics.
- Many tools like are not maintained and come with their own vulnerabilities.



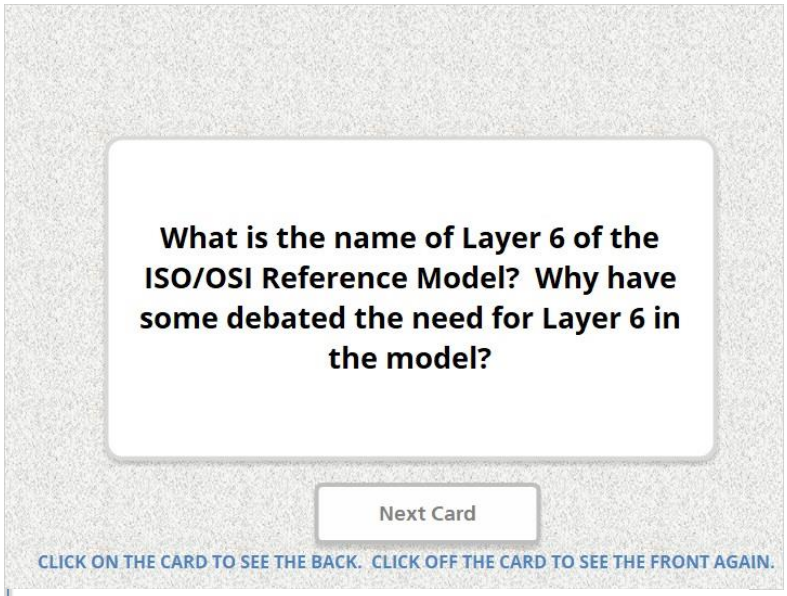


Transport Layer functions include:

Flow Control
Multiplexing
Virtual Circuit Management
Error Checking and Recovery



Session is a persistent logical linking of two software application processes. The **session layer** controls the dialogues (connections) between computers by providing the mechanism for opening, closing and managing a session between end-user application processes.

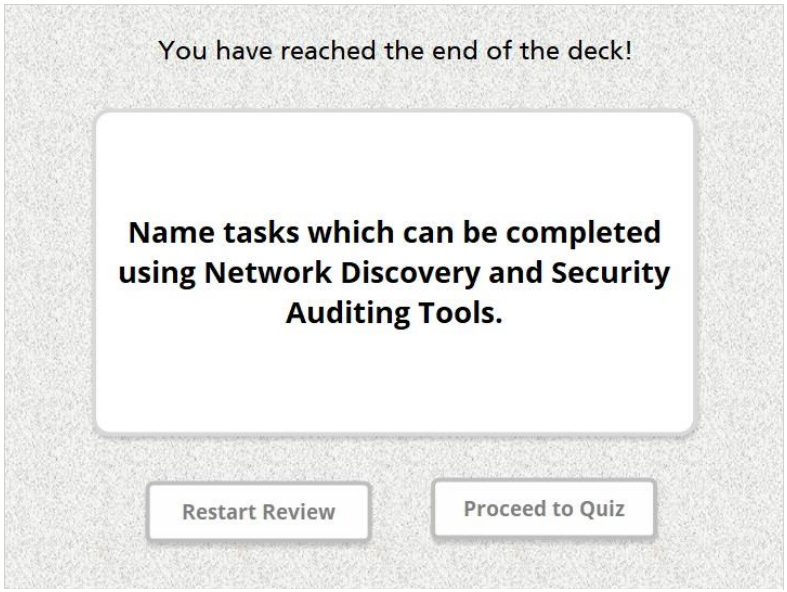


Layer 6 is the **Presentation Layer**.

This is an ambiguously defined layer and has been criticized formally many times and is debatable as a separate layer.

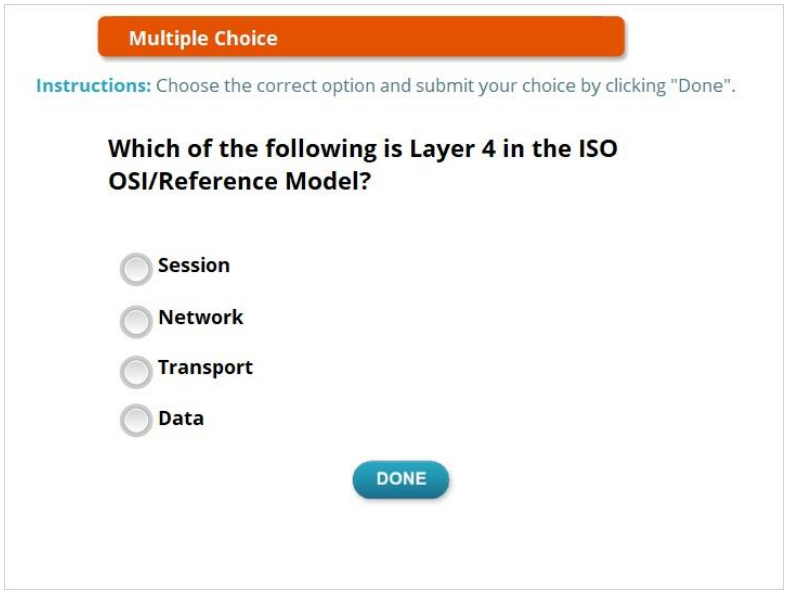
Most of the time its functions are carried out by protocols at other layers.

Application Layer protocols specify the rules to achieve specific tasks over a network. They interacts with software applications that implement a communicating component.

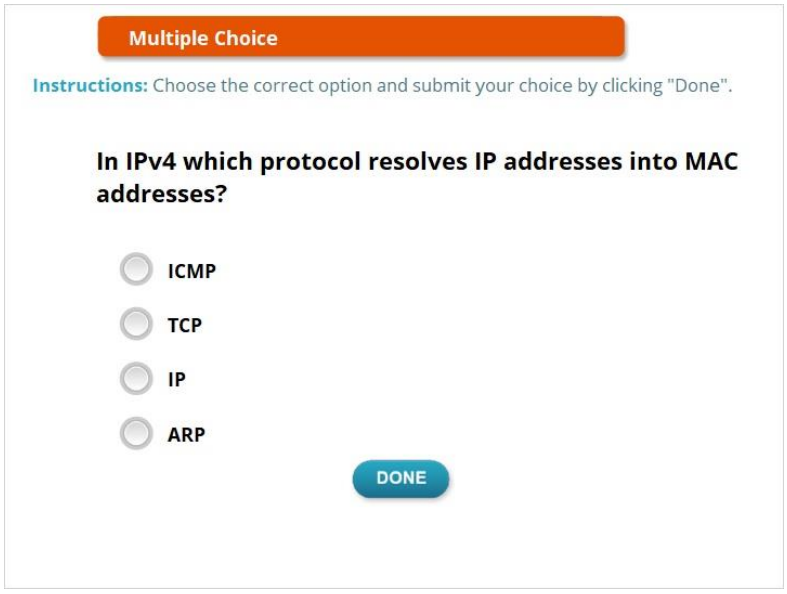


Many systems and network administrators find these tools useful for tasks such as **network inventory, managing service upgrade schedules, and monitoring host or service uptime.**

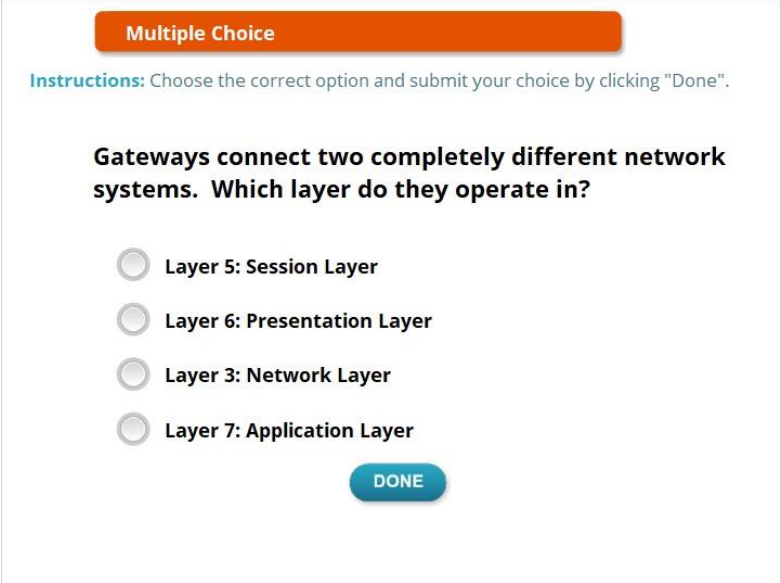
NOTE: These tools may also be used by unauthorized personnel.



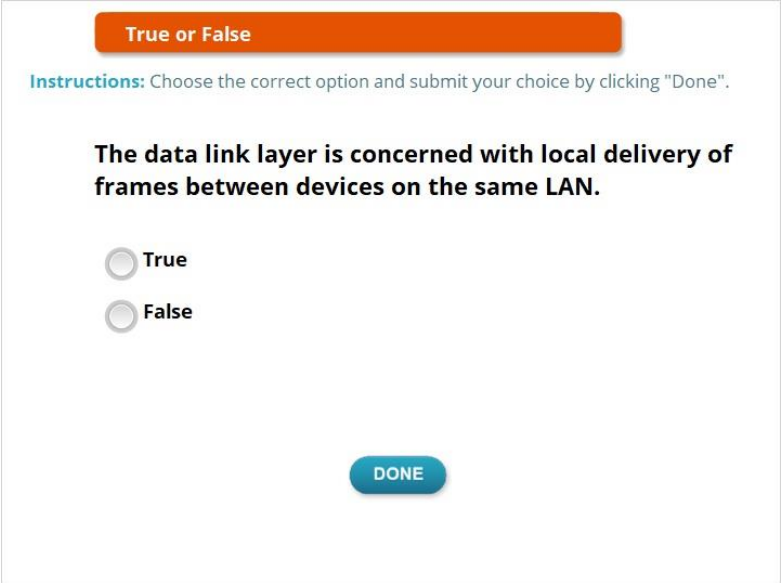
Correct	Choice
X	Radio Button 3



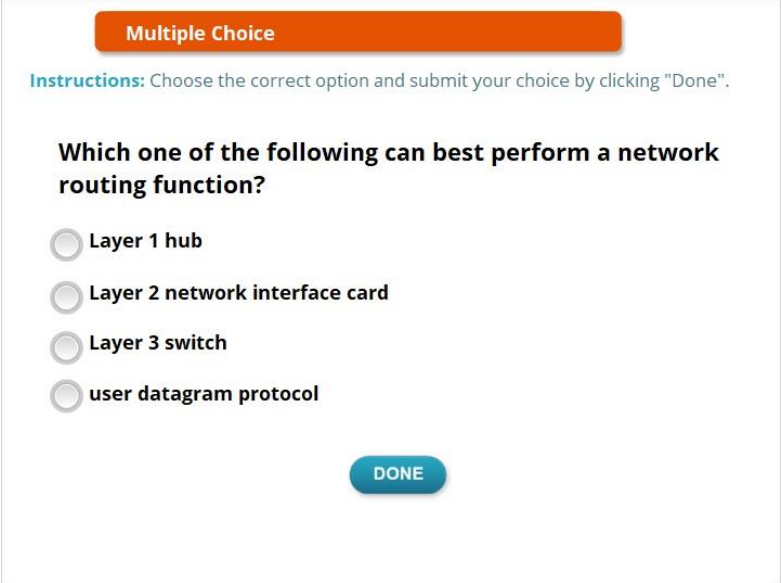
Correct	Choice
X	Radio Button 4



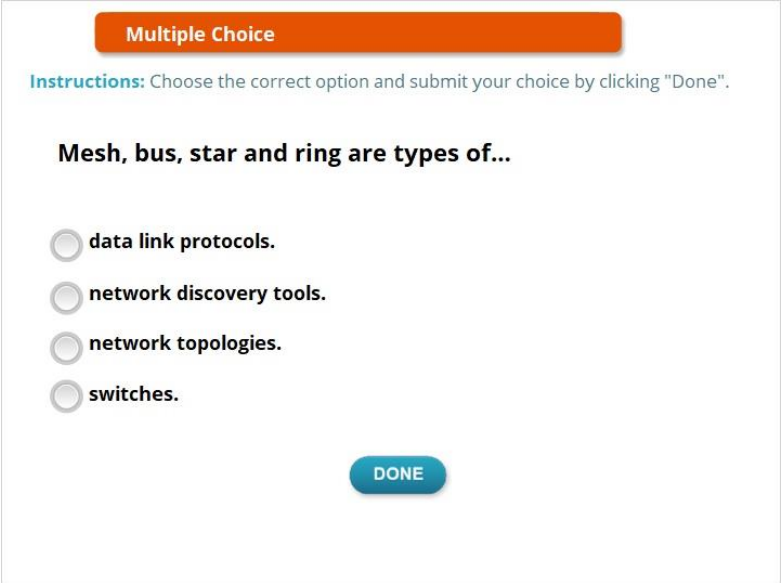
Correct	Choice
X	Radio Button 4



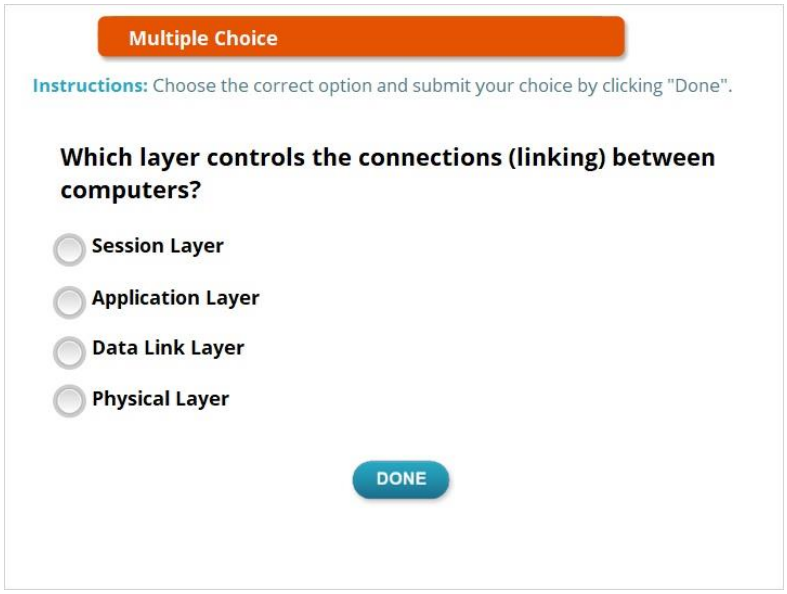
Correct	Choice
X	Radio Button 1



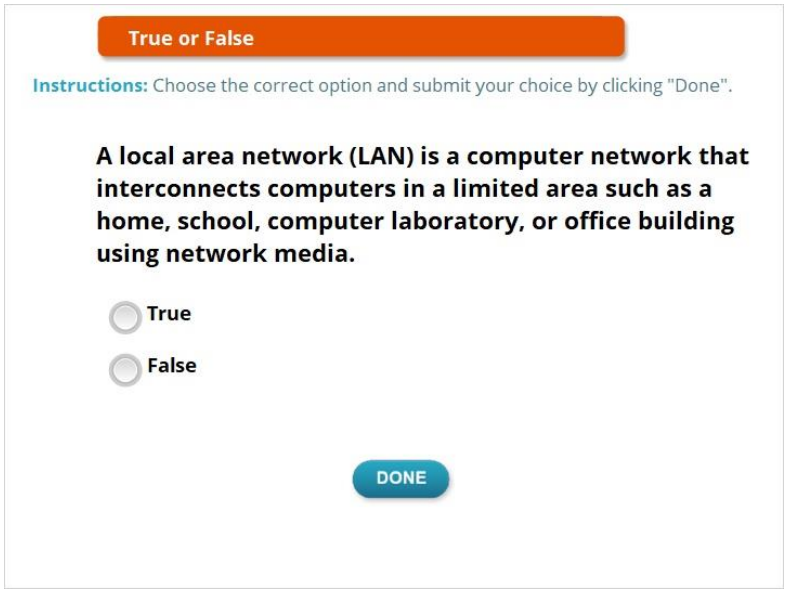
Correct	Choice
X	Radio Button 3



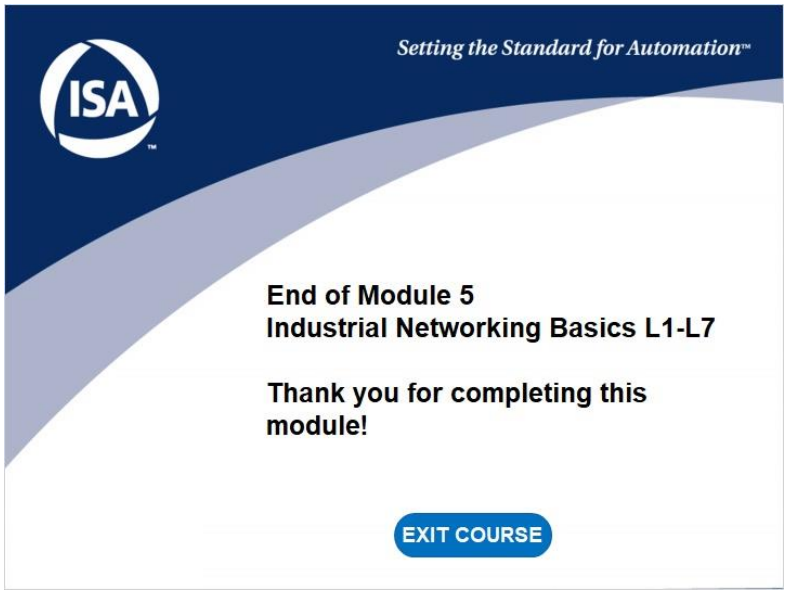
Correct	Choice
X	Radio Button 3



Correct	Choice
X	Radio Button 1



Correct	Choice
X	Radio Button 1


Setting the Standard for Automation™
End of Module 5
Industrial Networking Basics L1-L7
Thank you for completing this module!
EXIT COURSE

3.7 The Basic "Ethernet Design Rules"

The "5-4-3-2" rule states that the maximum transmission path is composed of 5 segments linked by 4 repeaters; the segments can be made of, at most, 3 coax segments with station nodes and 2 link [10BASE-FL] segments with no nodes between. Exceeding these rules means that some (though not all) nodes will be unable to communicate with some other nodes. You should check your design to ensure that no node is separated from any other node by more intermediate devices than the table below indicates.

Table 3-3. Maximum Transmission Path Between Any Two Nodes

5 segments 4 repeaters 3 link segments 2 coax segments	OR	5 segments 4 repeaters 3 coax segments 2 link segments

Note: This table is a popular simplification of the actual 802.3 rules.

3.8 "Would Somebody Please Explain This 7-Layer Networking Model?" (Adapted from *Sensors Magazine,* July 2001, ©Advanstar)

Networks, and the information that travels on them, are most easily understood in layers. For many years the International Standard Organization/Open Systems Interconnection (ISO/OSI) model (Figure 3-2) has been used as a way to represent the many layers of information in a network, particularly the low-level transport mechanisms. From top to bottom, these are the layers and how these layers relate to your product design (Table "Layer 1").

Please note that most networks do not actually use all these layers, only some. For example, Ethernet and RS-232 are just

physical layers—layer 1 only for RS-232 and layers 1 and 2 for Ethernet. TCP/IP is a protocol, not a network, and uses layers 3 and 4, regardless of whether layers 1 and 2 are a phone line, a wireless connection, or a 10BASE-T Ethernet cable.

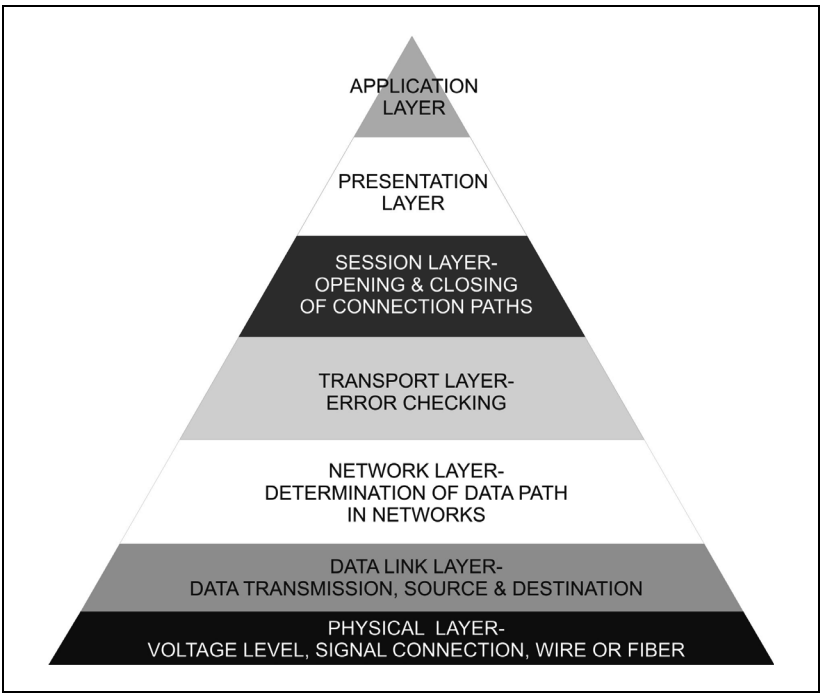


Figure 3-2. The 7-Layer Network Concept

Layer 7: Application

The application layer defines the meaning of the data itself. If you send me a .PDF file via email, the application that is used to open it is Adobe Acrobat. Many layers of protocols are involved, but the application is the final step in making the information usable.

In a sensor design, this is the software component that exchanges process data between the sensor elements (and their associated A/D converters, etc.) and the communications pro-

cessor. It recognizes the meaning of analog and digital values, parameters, and strings.

J1939 and CANopen are application layers on top of CAN. FOUNDATION Fieldbus HSE is an application layer on top of Ethernet and TCP/IP. Modbus is an application layer on top of RS-232/485.

Layer 6: Presentation

The presentation layer converts local data into a designated form for sending and for converting received data back to the local representation. It might convert a character set such as MacRoman to ASCII for transmission. Encryption can happen in this layer.

Layer 6 is usually handled by application software and is not usually used in industrial networks.

Layer 5: Session

The session layer creates and maintains communication channels (sessions). Security and logging can be handled here.

Layer 5 is handled by software and is not commonly used in industrial networks.

Layer 4: Transport

The transport layer controls transmission by ensuring end-to-end data integrity and by establishing the message structure protocol. It performs error checking.

Layer 4 is usually handled in software (e.g., TCP/IP).

Layer 3: Network

The network layer routes data from node to node in the network by opening and maintaining an appropriate path. It may also split large messages into smaller packets to be reassembled at the receiving end.

Layer 3 is done in software.

Layer 2: Data Link

The data link layer handles the physical transmission of data between nodes. A packet of data (data frame) has a checksum, source, and a destination. This layer establishes physical connection between the local machine and the destination, using the interface particular to the local machine.

Layer 2 is almost always done in hardware with application-specific integrated circuits (ASICs). Low-speed networks can perform layer 2 functions in software.

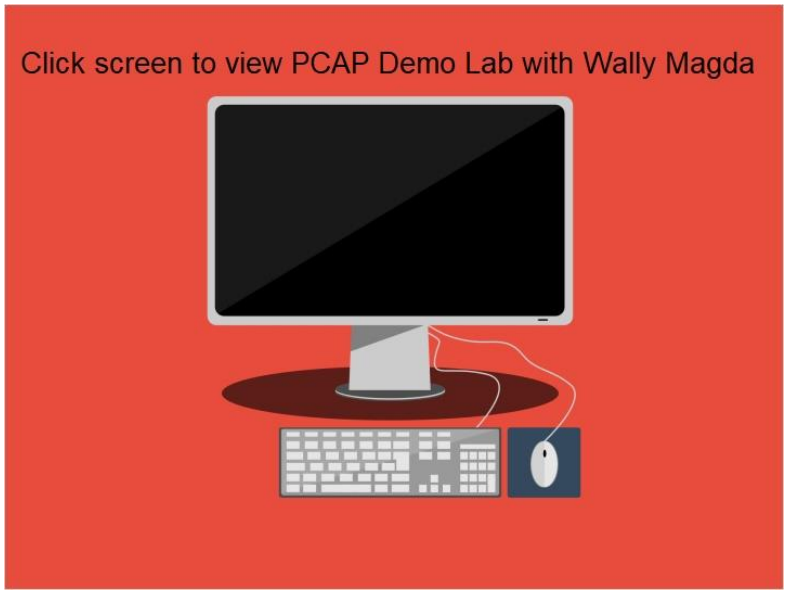
Layer 1: Physical Layer

Layer 1 defines signal voltages and physical connections for sending bits across a physical media and includes opto-isolation, hubs, and repeaters. Physical media refers to the tangible physical material that transports a signal, whether copper wire, fiber, or wireless.

The data to be transferred starts out in the application layer and is passed down the seven layers to the physical layer, where it is sent to the receiving system. At that end, it is passed up through the layers to the remote application layer, where it is finally received by the user.

IC329 Module 6

1.4 Lab Video



1.5 End of Module 6