DOWNLOAD PDF STANDARDS IN INFORMATION TECHNOLOGY AND INDUSTRIAL CONTROL

Chapter 1 : Cyber security standards - Wikipedia

Note: Citations are based on reference standards. However, formatting rules can vary widely between applications and fields of interest or study. The specific requirements or preferences of your reviewing publisher, classroom teacher, institution or organization should be applied.

History[edit] Cybersecurity standards have existed over several decades as users and providers have collaborated in many domestic and international forums to effect the necessary capabilities, policies, and practices - generally emerging from work at the Stanford Consortium for Research on Information Security and Policy in the s. TC CYBER is working closely with relevant stakeholders to develop appropriate standards to increase privacy and security for organisations and citizens across Europe. The committee is looking in particular at the security of infrastructures, devices, services and protocols, as well as security tools and techniques to ensure security. It offers security advice and guidance to users, manufacturers and network and infrastructure operators. Its standards are freely available on-line. A principal work item effort is the production of a global cyber security ecosystem of standardization and other activities. The latest versions of BS is BS The certification once obtained lasts three years. Depending on the auditing organisation, no or some intermediate audits may be carried out during the three years. The measurement standards are used for the static program analysis of software, a software testing practice that identifies critical vulnerabilities in the code and architecture of a software system. The Automated Source Code Security standard is a measure of how easily an application can suffer unauthorized penetration which may result in stolen information, altered records, or other forms of malicious behavior. The Automated Source Code Reliability standard is a measure of the availability, fault tolerance, recoverability, and data integrity of an application. The Reliability standard measures the risk of potential application failures and the stability of an application when confronted with unexpected conditions. Standard of Good Practice[edit] Main article: The ISF continues to update the SoGP every two years with the exception of ; the latest version was published in Originally the Standard of Good Practice was a private document available only to ISF members, but the ISF has since made the full document available for sale to the general public. Upon identification of a new patch, entities are required to evaluate applicability of a patch and then complete mitigation or installation activities within 35 calendar days of completion of assessment of applicability. These standards are used to secure bulk electric systems although NERC has created standards within other areas. The bulk electric system standards also provide network security administration while still supporting best-practice industry processes. It also emphasizes the importance of the security controls and ways to implement them. Initially this document was aimed at the federal government although most practices in this document can be applied to the private sector as well. Specifically it was written for those people in the federal government responsible for handling sensitive systems. It provides a high level description of what should be incorporated within a computer security policy. It describes what can be done to improve existing security as well as how to develop a new security practice. Eight principles and fourteen practices are described within this document. This document emphasizes the importance of self assessments as well as risk assessments. It allows many different software and hardware products to be integrated and tested in a secure way. The RFC provides a general and broad overview of information security including network security, incident response, or security policies. The document is very practical and focusing on day-to-day operations. This guidance applies to end-users i. Since , the committee has been developing a multi-part series of standards and technical reports on the subject of IACS security. They are also submitted to IEC for consideration as standards and specifications in the IEC series of international standards following the IEC standards development process. All ISA standards and technical reports are organized into four general categories called General, Policies and Procedures, System and Component. The second category of work products targets the Asset Owner. These address various aspects of creating and maintaining an effective IACS security program. The third category includes work products that describe system design guidance and requirements for the secure integration of control systems. Core in this is the zone and conduit design model. The fourth category includes work products that describe the specific product development and technical requirements of control system products. This is primarily intended for control product vendors, but can be used by integrator and asset owners for to assist in the procurement of secure products. The ISASecure scheme requires that all test tools be evaluated and approved to ensure the tools meet functional requirements necessary and sufficient to execute all required product tests and that test results will be consistent among the recognized tools. The certification labs must also meet ISO lab accreditation requirements to ensure consistent application of certification requirements and recognized tools. IEC [edit] The IEC cybersecurity standards are multi-industry standards listing cybersecurity protection methods and techniques. The comments are reviewed by various IEC committees where comments are discussed and changes are made as agreed upon. Each has defined their own scheme based upon the referenced standards and procedures which describes their test methods, surveillance audit policy, public documentation policies, and other specific aspects of their program. In the automation system market space most cybersecurity certifications have been done by exida. Global Accreditation and Recognition[edit] A global infrastructure has been established to ensure consistent evaluation per these standards. Certification Bodies are accredited to perform the auditing, assessment, and testing work by an Accreditation Body AB. There is often one national AB in each country. The IASME Governance standard was developed to enable businesses to achieve an accreditation similar to ISO but with reduced complexity, cost, and administrative overhead specifically focused on SME in recognition that it is difficult for small cap businesses to achieve and maintain ISO The cost of the certification is progressively graduated based upon the employee population of the SME e. Some insurance companies reduce premiums for cybersecurity related coverage based upon the IASME certification. The ANPR aims to enhance the ability of large, interconnected financial services entities to prevent and recover from cyber attacks, and goes beyond existing requirements.

Chapter 2 : Industrial & Technology Education - Career Technical Education (CA Dept of Education)

SPECIAL PUBLICATION REVISION 2 GUIDE TO INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY iii Reports on Computer Systems Technology The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST).

Todd Fitzgerald A variety of laws and regulations have surfaced over the past decade in an attempt to strengthen the security of information stored within the companies to which the information assets are entrusted. As a result of the laws and regulations, various security control "standards" and "frameworks" have evolved and become popular means to meet the requirements of the laws. Because laws and regulations are intentionally developed at a higher, "what needs to happen" level vs. Governance, risk, and compliance GRC is a term that has been embraced primarily by the vendor community in recent years in recognition of the fact that companies are struggling with the plethora of controls that must be implemented to meet the extensive requirements of the laws and regulations. Governance is simply the structure, policies, and practices that are put in place by the organization to ensure that the controls are adequately communicated, carried out, and enforced by engaging direction and support at the appropriate organizational level. Risk is the act of making informed decisions about the losses that the company is willing to accept given a breach of security and building the appropriate mitigating risk strategies to reduce the risk to acceptable levels defined by the business. Compliance is ensuring that the controls are being adhered to on an ongoing basis, thereby increasing the likelihood of a reduction of risk and increased adherence to the governance intended by the organization. The three components of GRC are necessary for adequate security controls; however, implementing them does not ensure that a security program is adequate. Compliance is a necessary control that has been recognized by governments for centuries. Criminal acts, by their very nature, are forms of noncompliance with the laws that are in place. Take driving a car for example. The teenager says, "Sure dad, no problem" and forgets five minutes later as he morphs into his busy teenage social network of friends and peer pressure, away from the constant parental reminders. He does not realize at the time the consequences of his actions. Or, maybe he does subconsciously, but it is not the most important thought in his daily "work life. The parent at that point transfers the risk to the child, and then the learning of true cost of noncompliance begins. The risk is ultimately acknowledged and accepted, and new mitigating strategies are put in place, such as better driving. Organizations are made up of many busy "teenagers," each of which is influenced by his peer work groups and needs to be educated as to the future costs of noncompliance to the security controls. Adopting a control framework is a good start; however compliance must be addressed as an ongoing, deliberate strategy. Control frameworks and security standards are often interchangeable terms depending upon the creator. COBIT defines a framework the same as a Control Framework, which is defined as a tool for business process owners that facilitates the discharge of their responsibilities through the provision of a supporting control model. Alternatively, COBIT defines a standard as a business practice or technology product that is an accepted practice endorsed by the enterprise or IT management team. These consist of documented, executed, tested, implemented, and monitored controls which reduce the risk of threats succeeding against the company vulnerabilities. The following are some examples of the control frameworks and standards that address information security requirements: The final rule for adopting security standards was published in February 20, , which required a series of administrative, technical, and physical security procedures for entities to use to assure the confidentiality of Protected Health Information PHI. The standard was intentionally non-technology specific and intended to provide scalability to small providers and large providers alike. The primary purpose is to provide a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets. The law also provided funding for NIST to develop the minimum necessary controls required to provide adequate security. The government publishes an annual report card based upon their assessment of compliance with the framework. The standards and guidelines reference the minimum set of controls that must be implemented to protect the federal system based upon the risk level determined. Implementation of the 17 families of security controls establishes a level of "security due diligence" for the federal agencies and the contractors which perform work for the government. These standards are very comprehensive, freely available, and an excellent resource to supplement the other control frameworks. Issued by the General Accounting Office, this provides guidance for Information Systems auditors to evaluate the IT controls used in support of financial statement audits. This is not an audit standard, but is included here because auditors are typically testing the control environment in government audits using this standard. Provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS. A framework and supporting toolset that allow managers to bridge the gap with respect to control requirements, technical issues and business risks, and communicate that level of control to stockholders. COBIT can be used to integrate other standards as an umbrella framework. COBIT gained increasing popularity through implementation to demonstrate compliance with Sarbanes-Oxley regulations, which were enacted in to require management and the external auditor to report on internal controls over financial reporting. A set of comprehensive requirements for enhancing payment account security, formed by several major credit card issuers, to facilitate the broad adoption of a comprehensive security standard. The framework contains a set of best practices for IT core operational processes such as change, release and configuration management, incident and problem management, capacity and availability management, and IT financial management. Configuration standards for Department of Defense Information Assurance, however freely available and used as the basis for technical standards for many private organizations. The World Operates on Standards The obvious fact about standards is that they are useful and the world is made up of many of them, from the minimum weight in the passenger seat that must be met before the airbag protection will become active, to the specification of the size of a 8 screw, to the standard formats for electronic data interchange of electronic transactions between healthcare providers, payers, and clearinghouses. Standards ensure that products are built to specifications and allow us to "simplify" the complexity of the world by creating a common deliverable and common language. Imagine if every time a manufacturer wanted a product built they had to design a screw that could be potentially different from any other screw a manufacturer created! Not only would this process be very expensive, it would also be very time consuming for the customer and the supplier, and would be very error-prone. Non-standardized processes also slow down the delivery of the product or service. Henry Ford recognized many years ago that there were efficiencies and increases in quality by creating vehicles which looked the same and were painted the same color black. While they were actually available in other colors, the primary color produced was black for efficiency. Imagine if stoplights were each made with different colors to represent stop-slowdown-go. Imagine roadways that used different types of striping to indicate passing vs. The world would be very chaotic with each individual interpreting the colors and passing lanes as they drove, many times potentially making the wrong decision. Sometimes we like the standards, sometimes we do not. Sometimes, they just do not make intuitive sense to us, nor do they seem effective. For example, the Transportation Security Administration TSA originally did not allow nail clippers on the airplane, and reversed the decision in after negative public opinion. Lighters were also subsequently allowed in July, by the Federal Aviation Administration. Laws, regulations, and the standards that support them are sometimes developed without the extensive analysis of their necessity, or in reaction to a major event and the need to "do something," only to be rescinded later for their lack of effectiveness. This is understood, as government and private industry must react to make demands and situations, making decisions on the data available at the time. In defense of the TSA, decisions to limit what was brought on an airplane had to be made quickly on the heels of September 11, , and their focus was on objects which had the potential to harm. Thus, the standard of "no nail clippers" was enacted. Liquid restrictions were placed on travelers due to an incident where the chemicals could be used to create explosives. By the time of this publication, due to new technology scanning, the "no liquid" standard may also disappear. Standards Are Dynamic Over time, the standards evolve, and they change to meet the societal and technological needs. While the intent of many security standards appears to stay the same over time, the underlying technologies that must be supported are constantly changing. Just as in the "no liquids" on airplanes were first introduced, and then evolved into "as long as the liquids are 3oz or less and fit in a 1qt baggie," and then may morph into "no requirements at all" due to investments in more advanced scanning technology, information security standards also need to change. Most control frameworks are written at a higher, broader level, which provides flexibility to implement controls to satisfy the specific technological request. For example, the ISO Before Hurricane Katrina inflicted extensive damage on New Orleans, Louisiana, and other surrounding areas in , many individuals felt that storage a few miles away was sufficient. Others have invested in new replication technologies and the availability of inexpensive storage to ensure availability of the information. Changing environments necessitate the ability to change the implementation strategies to meet the lower cost of technology, increased effectiveness of controls, and conformance to emerging regulations. The "How" Is Typically Left up to Us As the aforementioned example illustrates, the good news is that the standards may be written to be flexible over time. The bad news is that they are written to be flexible over time. In other words, standards often lack the specificity of the "how" that would be useful to implementing the standard. Obviously, this is by design; however, it leaves the implementer of the standard to "figure out" based upon the available alternatives what the best method of implementation should be for their particular environment and cost constraints. The "best practices" terminology has received criticism over the past several years, as the beauty is in the eye of the beholder. A practice that works for one organization may not fit for another. One organization may implement a policy banning USB drives due to their small size, while another may allow them as long as the contents are automatically encrypted with the company-approved software. Still another may prohibit their use by policy to most users, but allow adoption by those which establish a business need as specified in ISO Which is the "best practice"? It depends on the organizational culture, appetite for risk, cost constraints, etc. It may also be the case that the individuals within the organization do not have access to sensitive information, thus limiting the exposure. Therefore, the "best practice" for an organization must take in many factors not defined within the individual standard. Typically, an organization would be prudent to follow the trends within their particular vertical industry, and pay attention to what the "herd" is doing. Whatever these practices are named for our individual organizations, each must recognize that the practices must satisfy the standard and where they do not, sufficient business justification and risk acceptance must be documented. In this manner, the standards become the reference point for making informed business decisions. Why Does the Standard Exist? Before deciding the "how" to implement the standard, it is a useful exercise to examine the selected control within the standard and analyze why does this control exist in the first place? What threat is it addressing? What would the risk be to my organization if I decided to ignore addressing the control? In other words, how is implementing the control increasing the security, protection, or information assurance of the information assets within the organization? For example, if there is a control within the standard which says that logs of activity to the system must be retained for 1 year, access must be restricted to only those with a need to know, understanding why this standard exists will contribute to "how" it should be implemented. If the intent of the control is to be able to go back and analyze incidents, then the individuals who need read access are the systems security operations team, or those responding to the incidents. The files may also need to be online if there is a frequent occurrence of investigation. Alternatively, the logs may not be able to be reviewed due to resource human constraints, and may necessitate the investment in a security incident management tool which aggregates and correlates the information. Understanding the intent of the control also assists in interpreting the terminology used within the control. The standards are promulgated by many different organizations, committees, and geographic representations. The NIST uses terminology in the standard Recommended Security Controls for Federal Information Systems with roots in the Government Sector that would be familiar to many accustomed to working for or contracting with government agencies. The danger in this is that the security controls implemented may prove to be ineffective to addressing the vulnerabilities of the organization and the threats that they face. However, even though compliance with standards may not be sufficient to mitigate the risk level to an acceptable level for the organization, the fact that the organization is adopting a control framework provides the opportunity to create a baseline and enhance the security level over time. Without such a framework in place, there is less chance that the environment will be secure, as items can be missed too easily. Integration of Standards and Control Frameworks Each of the standards and control frameworks contributes in their own way and the astute security professional will become familiar with each of them.

Chapter 3 : - Information technology (IT) in general

Standards in Information Technology and Industrial Control (Malagardis) () ISBN: - pp., hardcover, ex library but text & binding clean & tight.

Chapter 4 : Leveraging IT Control Frameworks for Compliance

Many manufacturing organizations leverage industrial control systems (ICS) to monitor and control physical processes. As ICS continue to adopt standard commercial information technology (IT) solutions to promote corporate business systems connectivity and remote access capabilities, ICS become more.

Chapter 5 : Majoring in Quality Control Technology: What is Included in this Major?

Enter your mobile number or email address below and we'll send you a link to download the free Kindle App. Then you can start reading Kindle books on your smartphone, tablet, or computer - no Kindle device required.

Chapter 6 : NIST: National Institute of Standards and Technology

Information and Communication Technology (ICT) Standards The Information Technology Laboratory (ITL), one of seven research laboratories within the National Institute of Standards and Technology (NIST), is a globally recognized and trusted source of high-quality.

Chapter 7 : List of technical standard organisations - Wikipedia

Papua New Guinea â€” NISIT â€” National Institute of Standards and Industrial Technology Peru â€” INDECOPI â€” Instituto Nacional de Defensa de la Competencia y de la ProtecciÃ³n de la Propiedad Intellectual.

Chapter 8 : Standards in Information Technology Industrialâ€¦ -

The International Organization for Standardization (ISO) offering standards for agricultural product, telecommunications, Railway, Testing, healthcare technology and safety, Medical equipment, heat pumps, information technology, manufacturing industry and many more.

Chapter 9 : ISO Standards for Information Technology, Manufacturing Industry

The National Institute of Standards and Technology (NIST) has issued the second revision to its Guide to Industrial Control Systems (ICS) Security. It includes new guidance on how to tailor traditional IT security controls to accommodate unique ICS performance, reliability and safety requirements.