
Leading Resources to support your Information Security improvement efforts

The Computer Security Division (CSD) of the National Institute of Standards and Technology (NIST), including the Federal Information Security Management Act (FISMA) library.

The mission of NIST's Computer Security Division is to improve information systems security by:

- Raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies;
- Researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive Federal systems;
- Developing standards, metrics, tests and validation programs:
 - to promote, measure, and validate security in systems and services
 - to educate consumers and
 - to establish minimum security requirements for Federal systems
- Developing guidance to increase secure IT planning, implementation, management and operation.

<http://csrc.nist.gov/>

<http://csrc.nist.gov/sec-cert/ca-library.html>

Build Security In (BSI)

As part of the Software Assurance program, Build Security In (BSI) is a project of the Strategic Initiatives Branch of the National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS). The Software Engineering Institute (SEI) was engaged by the NCSD to provide support in the Process and Technology focus areas of this initiative. The SEI team and other contributors develop and collect software assurance and software security information that helps software developers, architects, and security practitioners to create secure systems.

<https://buildsecurityin.us-cert.gov/daisy/bsi/home.html>

CERT[®]'s Resiliency Engineering Research

The cornerstone of their research is the development of the CERT[®] Resiliency Engineering Framework. The framework is the foundation for a process improvement approach to security and business continuity. It establishes an organization's resiliency engineering process: a collection of essential capabilities that an organization performs to ensure that its important assets—people, information, technology, and facilities—stay productive in supporting business processes and services. The framework serves as a foundation from which an organization can measure its current competency, set improvement targets, and establish plans and actions to close any identified gaps. As a result, the organization repositions and repurposes its security and business continuity activities and takes on a process improvement mindset that helps to keep these activities productive in the long run.

http://www.cert.org/resiliency_engineering/

The **Center for Internet Security (CIS)** is a non-profit enterprise whose mission is to help Organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls. CIS members develop and encourage the widespread use of security configuration benchmarks through a global consensus process involving participants from the public and private sectors. The practical CIS Benchmarks support available high level standards that deal with the "Why, Who, When, and Where" aspects of IT security by detailing "How" to secure an ever widening array of workstations, servers, network devices, and software applications in terms of technology specific controls. CIS Scoring Tools analyze and report system compliance with the technical control settings in the Benchmarks. The CIS Benchmarks and Scoring Tools are available for download free of charge.

<http://www.cisecurity.org/index.html>

Process Agnostic Navigational View

The process agnostic approach incorporates security into each basic phase of software development. The best practices and methods described are applicable to any and all development approaches as long as they result in the creation of software artifacts.

<https://buildsecurityin.us-cert.gov/daisy/bsi/438.html>

Governing for Enterprise Security Implementation Guide

This guidance is designed to help business leaders implement an effective program to govern information technology (IT) and information security.

<http://www.cert.org/governance/ges.html>

- [Article 1: Characteristics of Effective Security Governance \(pdf\)](#)
- [Article 2: Defining an Effective Enterprise Security Program \(ESP\) \(pdf\)](#)
- [Article 3: Enterprise Security Governance Activities \(pdf\)](#)

ISO27001 in North America

ISO27001 is the new, international standard of information security best practice. With its origins in ISO17799 and BS7799, ISO27001 is providing comprehensive best-practice advice and guidance to private and public sector organizations around the world on how to design and implement an effective information security management system ('ISMS'). On this site, you can find out how an **ISO27001 ISMS** can help organizations meet their commercial and business needs for cost-effective information security while at the same meeting their information- related **regulatory compliance** objectives and positioning them for new and emerging regulations.

<http://www.27001.com/default.aspx>

The Defense-in-Depth Foundational Curriculum handbook discusses information assurance issues and how to address these at both organizational and technical levels. The handbook is written for students ranging from system administrators to CIOs who have some technical understanding of information systems.

http://www.cert.org/archive/pdf/Defense_in_Depth092106.pdf

Guide 6: Managing and Auditing IT Vulnerabilities

The IIA has released its sixth guide in its Global Technology Audit Guide (GTAG®) series, *Managing and Auditing IT Vulnerabilities*. The 24-page guide was developed to help CAEs and internal auditors ask the right questions of IT security staff when assessing the effectiveness of their vulnerability management processes. The guide recommends specific management practices to help an organization achieve and sustain higher levels of effectiveness and efficiency and illustrates the differences between high- and low-performing vulnerability management efforts.

<http://www.theiia.org/guidance/technology/gtag/gtag6/>

The (ISC)² 2007 Resource Guide for Today's Information Security Professional - Global Edition - provides the latest resources in educational references, year-long events listings and leading industry sponsors all in one handy downloadable reference guide.

<https://www.isc2.org/cgi-bin/content.cgi?page=920>

Security Configuration Checklists Program for IT Products

A security configuration checklist (sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration) is essentially a document that contains instructions or procedures for configuring an IT product to a baseline level of security.

<http://checklists.nist.gov/index.html>

Ask the Auditor: Who is Responsible for Information Security?

The Auditor Responds: In short, the board of directors, management (of both staff and business lines), and internal audit functions all have significant roles in auditing information security. The big question for many companies is how these stakeholders should work together to ensure that everything that should be done to protect sensitive data is being done—and that the company's key assets are protected appropriately.

<http://www.itcinstitute.com/display.aspx?id=1823>

National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) – (See below for their key initiatives) - <http://csrc.nist.gov/>

a) US Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems" (PDF): <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>

b) NIST Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems" (PDF): <http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf>

c) NIST Special Publication (SP) 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems" (PDF): <http://csrc.nist.gov/publications/drafts/SP800-53A-spd.pdf>

d) Federal Information Security Management Act (FISMA) Implementation Project: <http://csrc.nist.gov/sec-cert/>

Schaser-Vartan Books' new release, **Say What You Do**, spells out in layman's terms the often bewildering differences between [policies](#), procedures and standards — topics that have historically been written about in industry jargon. What sets the book apart is its candidly practical approach, focusing on creating policies that really work rather than pushing theories that break down in the real world. "Armed with this book, you should be able to lead a policy development project at your company from the ground up and from the top down without losing your mind," says co-author and attorney Marcelo Halpern.

http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20070417005246&newsLang=en

How to establish an effective Computer Security Incident Response Team at:

<http://www.cert.org/csirts>

Auditing BCP and DR efforts - THE resource repository.

Various leading resources to support the auditing of BCP and DR programs.

<http://www.auditnet.org/drp.htm>

IT Compliance Institute (ITCi) – “IT Audit Checklist for Information Security”.

This paper, *IT Audit Checklist: Information Security*, supports an internal audit of the organization's information security program with guidance on improving information security programs and processes, as well as information on assessing the robustness of your organization's security efforts. The paper is intended to help IT, compliance, audit, and business managers prepare for an audit of information security and, ultimately, to ensure that the audit experience and results are as productive as possible.

<http://www.itcinstitute.com/info.aspx?id=34985>

What the Board Needs to Know About IT: Phase II Findings

Maximizing performance through IT strategy

<http://www.deloitte.com/dtt/article/0,1002,sid=36692&cid=151800,00.html>

ISO 27001 CERTIFICATION GUIDES LAUNCHED

IT Governance Ltd has launched the world's first practical guides to help company directors and IT project managers understand and achieve certification to ISO 27001, the newly published global certification standard for information security management (replaces BS7799 and complements ISO 17799). In the modern corporate governance climate, ISO 27001 certification will increasingly become a prerequisite for winning new business, thereby accelerating the transfer of IT security issues from the data room to the boardroom.

http://www.itgovernance.co.uk/news_detail.aspx?news_id=25

What the Board Needs to Know About IT (The board's role in leveraging technology as a strategic resource)

In 2006, Deloitte Consulting LLP began a research initiative to explore how boards of directors are approaching information technology (IT). Phase I of this research represents the findings of more than 30 interviews with directors and senior executives. The findings from the Phase I interviews have been captured in the point of view: "[What the Board Needs to Know About IT: The Board's Role in Leveraging Technology as a Strategic Resource](#)."

You can also download "[Bringing IT Into the Boardroom](#)," which appeared as a supplement to the Fall 2006 issue of *Corporate Board Member* magazine. Finally, you can learn about the upcoming Phase II research results on the topic of the board and IT by downloading a preview of the survey results, entitled: "[Big Conundrum: Phase II Preliminary Findings](#)."

For more info on the Deloitte initiative, all the above mentioned documents, and "more", visit:

<http://www.deloitte.com/dtt/article/0,1002,sid%3D26562%26cid%3D132853,00.html>

CERT Launches Podcast Series

The CERT® Program is pleased to announce the launch of its first podcast series, "Security for Business Leaders," available at <http://www.cert.org/podcast>. The series will provide both general principles and specific starting points for

business leaders who want to launch enterprise-wide security efforts, or who want to ensure that their organizations' existing security program is as effective as possible. New podcasts will be available every two weeks. The newest podcast features Rich Pethia, Director of the CERT Program. Other podcast topics include "Why Leaders Should Care about Security," "The ROI of Security," "Proactive Remedies for Rising Threat," and "Compliance vs. Buy-in." Podcasters can listen to entire conversations, download PDF transcripts, and investigate additional references in show notes.

["Security for Business Leaders"](#) is the first podcast series for the SEI.

The Language of Compliance

The Language of Compliance is the biggest (3,500+ entries) resource for acronyms, terms, and extended definitions. Authored by Dorian Cougias and Marcelo Halpern it covers the terms found in HIPAA, SOX, GLB, CobiT, ISO 17799 and 27001, BCI, BSI, ISSF, and over 100 other regulatory bodies and standards agencies.

http://glossary.unifiedcompliance.com/buy_now/the_language_of_compliance.html

Unified Compliance Project (UCP)

ITCi's Unified Compliance Project (UCP) is an independent initiative focused on supporting IT compliance management. The UCP parses and reconstructs complex corporate regulations into a holistic IT compliance view.

<http://www.itcinstitute.com/ucp/>

Global Technology Audit Guide (GTAG)

The Institute of Internal Auditors (The IIA) is producing a series of publications with guidance on information technology. Written primarily for the chief internal audit executive (CAE) and audit supervisors, the guides address concerns of the board of directors and chief-level executives. Each Global Technology Audit Guide (GTAG) is written in straightforward business language to address timely issues related to information technology management, control, or security. GTAG is a ready resource series for chief audit executives to use in the education of members of the board and audit committee, management, process owners, and others regarding technology-associated risks and recommended practices.

<http://www.theiia.org/guidance/technology/gtag/>

Avoiding IS Icebergs

This article explores the audit's assurance role regarding information security and outlines approaches and methodologies. The article is targeted to the beginner infosec professional, though more experienced practitioners will also find it useful as an update on what's available and in use today.

<http://infosecuritymag.techtarget.com/articles/october00/features3.shtml>

The British Columbia provincial information security policy (its their security handbook).

The B.C. provincial government has issued a first draft of their information security policy and welcomes any and all comments and suggestions (to improve it).

<http://www.cio.gov.bc.ca/prgs/ManualInformationSecurityPolicyV1.pdf>

IT Compliance Institute (ITCi) – "IT Audit Checklist for Risk Management".

Are you prepared for your next risk management audit? Know what to expect.

Note – a brief registration is required (to download the free white paper).

<http://www.itcinstitute.com/display.aspx?id=2499>

Keeping Up Your SOX Compliance and Turning IT into a High Performer by Improving Change Control. Study the extensive benefits of establishing a robust change management and change auditing practices including the latest research by ITPI (IT Process Institute).

http://www.tripwire.com/resources/asset_request.cfm?aid=2184

Managing Enterprise Risk in Today's World of Sophisticated Threats: A Framework for Developing Broad-Based, Cost-Effective Information Security Programs

<http://csrc.nist.gov/sec-cert/rmf-sz.pdf>

Other **NIST white papers** - csrc.nist.gov/sec-cert/ca-library.html#fisma-white-paper

The IT Process Improvement Institute

The IT Process Institute (ITPI) is an independent research organization that exists to support the professional communities of IT audit, security, and operations professionals. They are dedicated to working with IT leaders to advance the science of IT management. The IT Process Institute has created a unique three-part methodology designed to create and share results-oriented prescriptive guidance with our members including: 1) Research - study top performers and identify the causal link between behavior and results; 2) Benchmarking - create tools that compare individual organizations to top performers; and 3) Prescriptive Guidance - share content written to help IT organizations become top performers. Their latest benchmarking study results are also truly “insightful” – go to the second link for free access to the “Executive Overview”.

<http://www.itpi.org/home/default.php> and http://www.itpi.org/home/wp_reg.php

Auditing IT Initiatives - Because an IT Project Failure is NOT An Option.

Key questions to consider:

- Does the proposed IT solution work & will it meet the needs of the organization?
- Does the security aspect of the IT solution work?
- Will the privacy of the organization’s information be maintained?
- Will the staff know how to perform “productively” and accurately?
- Have we done everything necessary to be prepared?
- Are we ready to implement and how do you know it’ll work?

<http://www.auditnet.org/articles/DSIA200702.htm>

The Visible Ops Handbook

Visible Ops: Starting ITIL in four practical and auditable steps – is getting rave reviews. If you need practical guidance on how to jumpstart ITIL or IT control projects – this book is for you. Get control of your infrastructure; increase security, auditability, and service levels; decrease costs.

<http://www.itpi.org/home/visibleops2.php>