NIST Special Publication 800-12
Revision 1

An Introduction to Information Security

Michael Nieles
Kelley Dempsey
Victoria Yan Pillitteri

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-12r1

COMPUTER SECURITY

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-12
Revision 1

An Introduction to Information Security

Michael Nieles
Kelley Dempsey
Victoria Yan Pillitteri
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-12r1

June 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-12 Revision 1
Natl. Inst. Stand. Technol. Spec. Publ. 800-12 Rev. 1, 101 pages (June 2017)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-12r1

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: sec-cert@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in systems security as well as its collaborative activities with industry, government, and academic organizations.

Abstract

Organizations rely heavily on the use of information technology (IT) products and services to run their day-to-day activities. Ensuring the security of these products and services is of the utmost importance for the success of the organization. This publication introduces the information security principles that organizations may leverage to understand the information security needs of their respective systems.

Keywords

assurance; computer security; information security; introduction; risk management; security controls; security requirements

Acknowledgements

The authors would like to thank everyone who took the time to review and make comments on the draft of this publication, specifically Celia Paulsen, Ned Goren, Isabel Van Wyk, and Rathini Vijayaverl of the National Institute of Standards and Technology (NIST). The authors would also like to acknowledge the original authors, Barbara Guttman and Edward A. Roback, as well as all those individuals who contributed to the original version of this publication.

Table of Contents

1 Introduction 1
1.1 Purpose 1
1.2 Intended Audience 1
1.3 Organization 1
1.4 Important Terminology 2
1.5 Legal Foundation for Federal Information Security Programs 3
1.6 Related NIST Publications 4
2 Elements of Information Security 7
2.1 Information security supports the mission of the organization 7
2.2 Information security is an integral element of sound management 8
2.3 Information security protections are implemented so as to be commensurate with risk 8
2.4 Information security roles and responsibilities are made explicit 9
2.5 Information security responsibilities for system owners go beyond their own organization 9
2.6 Information security requires a comprehensive and integrated approach 9
2.6.1 Interdependencies of security controls 10
2.6.2 Other interdependencies 10
2.7 Information security is assessed and monitored regularly 10
2.8 Information security is constrained by societal and cultural factors 11
3 Roles and Responsibilities 13
3.1 Risk Executive Function (Senior Management) 13
3.2 Chief Executive Officer (CEO) 13
3.3 Chief Information Officer (CIO) 14
3.4 Information Owner/Steward 14
3.5 Senior Agency Information Security Officer (SAISO) 14
3.6 Authorizing Official (AO) 15
3.7 Authorizing Official Designated Representative 15
3.8 Senior Agency Official for Privacy (SAOP) 15
3.9 Common Control Provider 15
3.10 System Owner 16
3.11 System Security Officer (SSO) 16

3.12 Information Security Architect 16
3.13 System Security Engineer (SSE) 17
3.14 Security Control Assessor 17
3.15 System Administrator 17
3.16 User 17
3.17 Supporting Roles 18
4 Threats and Vulnerabilities: A Brief Overview 20
4.1 Examples of Adversarial Threat Sources and Events 20
4.1.1 Fraud and Theft 21
4.1.2 Insider Threat 22
4.1.3 Malicious Hacker 22
4.1.4 Malicious Code 23
4.2 Examples of Non-Adversarial Threat Sources and Events 24
4.2.1 Errors and Omissions 24
4.2.2 Loss of Physical and Infrastructure Support 24
4.2.3 Impacts to Personal Privacy of Information Sharing 25
5 Information Security Policy 26
5.1 Standards, Guidelines, and Procedures 26
5.2 Program Policy 27
5.2.1 Basic Components of Program Policy 27
5.3 Issue-Specific Policy 28
5.3.1 Example Topics for Issue-Specific Policy 28
5.3.2 Basic Components of Issue-Specific Policy 29
5.4 System-Specific Policy 30
5.4.1 Security Objectives 31
5.4.2 Operational Security Rules 31
5.4.3 System-Specific Policy Implementation 32
5.5 Interdependencies 32
5.6 Cost Considerations 33
6 Information Security Risk Management 34
6.1 Categorize 36
6.2 Select 36

6.3 Implement 37
6.4 Assess 37
6.5 Authorize 37
6.6 Monitor 37
7 Assurance 38
7.1 Authorization 38
7.1.1 Authorization and Assurance 39
7.1.2 Authorization of Products to Operate in Similar Situation 39
7.2 Security Engineering 39
7.2.1 Planning and Assurance 39
7.2.2 Design and Implementation Assurance 39
7.3 Operational Assurance 41
7.3.1 Security and Privacy Control Assessments 42
7.3.2 Audit Methods and Tools 42
7.3.3 Monitoring Methods and Tools 44
7.4 Interdependencies 46
7.5 Cost Considerations 46
8 Security Considerations in System Support and Operations 47
8.1 User Support 47
8.2 Software Support 48
8.3 Configuration Management 48
8.4 Backups 49
8.5 Media Controls 49
8.6 Documentation 49
8.7 Maintenance 50
8.8 Interdependencies 50
8.9 Cost Considerations 51
9 Cryptography 52
9.1 Uses of Cryptography 52
9.1.1 Data Encryption 52
9.1.2 Integrity 53
9.1.3 Electronic Signatures 53

9.1.4 User Authentication 54

9.2 Implementation Issues 54

9.2.1 Selecting Design and Implementation Standards 55

9.2.2 Deciding between Software, Hardware, or Firmware Implementations 55

9.2.3 Managing Keys 55

9.2.4 Security of Cryptographic Modules 56

9.2.5 Applying Cryptography to Networks 56

9.2.6 Complying with Export Rules 57

9.3 Interdependencies 57

9.4 Cost Considerations 58

9.4.1 Direct Costs 58

9.4.2 Indirect Costs 58

10 Control Families 59

10.1 Access Control (AC) 59

10.2 Awareness and Training (AT) 59

10.3 Audit and Accountability (AU) 60

10.4 Assessment, Authorization, and Monitoring (CA) 60

10.5 Configuration Management (CM) 61

10.6 Contingency Planning (CP) 61

10.7 Identification and Authentication (IA) 62

10.8 Individual Participation (IP) 63

10.9 Incident Response (IR) 64

10.10 Maintenance (MA) 64

10.11 Media Protection (MP) 65

10.12 Privacy Authorization (PA) 65

10.13 Physical and Environmental Protection (PE) 66

10.14 Planning (PL) 67

10.15 Program Management (PM) 67

10.16 Personnel Security (PS) 68

10.17 Risk Assessment (RA) 68

10.18 System and Services Acquisition (SA) 69

10.19 System and Communications Protection (SC) 69

10.20 System and Information Integrity (SI) 70

List of Appendices

Appendix A— References 71

Appendix B— Glossary 76

Appendix C— Acronyms and Abbreviations 88

List of Figures

Figure 1 - Risk Management Framework (RMF) Overview 36