ASIS INTERNATIONAL

Auditing Management Systems:

Risk, Resilience, Security, and Continuity—Guidance for Application

ANSI/ASIS SPC.2-2014

STANDARD

The worldwide leader in security standards and guidelines development

ASIS INTERNATIONAL
Advancing Security Worldwide®

ANSI/ASIS SPC.2-2014

an American National Standard

AUDITING MANAGEMENT SYSTEMS: RISK, RESILIENCE, SECURITY, AND CONTINUITY—GUIDANCE FOR APPLICATION

Approved March 28, 2014

American National Standards Institute, Inc.

ASIS International

Abstract

This *Standard* provides guidance for conducting resilience, security, crisis, continuity and other risk based audits within the context of management systems and includes practical advice on conducting audits. It provides guidance on the management of audit programs, conduct of internal or external audits of risk and resilience based management systems such as security, crisis, continuity, and emergency management, including the competence and evaluation of auditors.

Notice and Disclaimer

The information in this publication was considered technically sound by the consensus of those who engaged in the development and approval of the document at the time of its creation. Consensus does not necessarily mean that there is unanimous agreement among the participants in the development of this document.

ASIS International standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest and knowledge in the topic covered by this publication. While ASIS administers the process and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

ASIS is a volunteer, nonprofit professional society with no regulatory, licensing or enforcement power over its members or anyone else. ASIS does not accept or undertake a duty to any third party because it does not have the authority to enforce compliance with its standards or guidelines. It assumes no duty of care to the general public, because its works are not obligatory and because it does not monitor the use of them.

ASIS disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. ASIS disclaims and makes no guaranty or warranty, expressed or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any person's or entity's particular purposes or needs. ASIS does not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, ASIS is not undertaking to render professional or other services for or on behalf of any person or entity, nor is ASIS undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

ASIS has no power, nor does it undertake to police or enforce compliance with the contents of this document. ASIS has no control over which of its standards, if any, may be adopted by governmental regulatory agencies, or over any activity or conduct that purports to conform to its standards. ASIS does not list, certify, test, inspect, or approve any practices, products, materials, designs, or installations for compliance with its standards. It merely publishes standards to be used as guidelines that third parties may or may not choose to adopt, modify or reject. Any certification or other statement of compliance with any information in this document should not be attributable to ASIS and is solely the responsibility of the certifier or maker of the statement.

ISBN: 978-1-934904-55-8

FOREWORD

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the *Standard*.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

This conformity assessment standard provides generic auditable criteria and informative guidance.

About ASIS

ASIS International (ASIS) is the leading organization for security professionals, with more than 38,000 members worldwide. ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, government entities, and the public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's No. 1 magazine – *Security Management* - ASIS leads the way for advanced and improved security performance.

The work of preparing standards and guidelines is carried out through the ASIS International Standards and Guidelines Committees, and governed by the ASIS Commission on Standards and Guidelines. An ANSI accredited Standards Development Organization (SDO), ASIS actively participates in the International Organization for Standardization. The Mission of the ASIS Standards and Guidelines Commission is *to advance the practice of security management through the development of standards and guidelines within a voluntary, nonproprietary, and consensus-based process, utilizing to the fullest extent possible the knowledge, experience, and expertise of ASIS membership, security professionals, and the global security industry.*

Suggestions for improvement of this document are welcome. They should be sent to ASIS International, 1625 Prince Street, Alexandria, VA 22314-2818, USA.

Commission Members

Charles A. Baley, Farmers Insurance Group, Inc.
Jason L. Brown, Thales Australia
Michael Bouchard, Sterling Global Operations, Inc.
Cynthia P. Conlon, CPP, Conlon Consulting Corporation
William J. Daly, Control Risks Security Consulting
Lisa DuBrock, Radian Compliance
Eugene F. Ferraro, CPP, PCI, CFE, Convercent
F. Mark Geraci, CPP, Purdue Pharma L.P.
Bernard D. Greenawalt, CPP, Securitas Security Services USA, Inc.
Robert W. Jones, Socrates Ltd
Glen Kitteringham, CPP, Kitteringham Security Group Inc.
Michael E. Knoke, CPP, Express Scripts, Inc.
Bryan Leadbetter, CPP, CISSP
Marc H. Siegel, Ph.D., ASIS International, European Bureau
Jose Miguel Sobron, United Nations
Roger D. Warwick, Pyramid International

Allison Wylde, Researcher and Consultant

At the time it approved this document, the SPC.2 Standards Committee, which is responsible for the development of this *Standard*, had the following members:

Committee Members

Committee Chair: Marc H. Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative
Commission Liaison: Lisa DuBrock, CPA, CBCP, MBCI, Radian Compliance, LLC
Committee Secretariat: Susan Carioti, ASIS International

Sean Ahrens, M.A., CPP, BSCP, CSC, Aon Risk Services
Mitchell Albinski, Blackhall River Security Associates
Lyle Alexander, CPP, A.R.M Specialists Ltd
Kourosh Aliha, CFI, Independent
Frank Amoyaw, LandMark Security Limited
Dennis Arter, ASQ Fellow, Certified Quality Auditor, American Society for Quality
Abrar Ashraf, CPP, PSP, Secure Options Group
Paul Aube, CPP, Dessau
Mark Baker, CPP, MBaker Security
Jay Beighley, CPP, Nationwide Insurance
Frank Bellomo, Business Risks International Pty. Limited
Gil BevenFlorez Jr., Independent
Albert Senior Security Consultant
Dennis Blass, CPP, PSP, CFE, CISSP, CHSP, Children's of Alabama
Terry Blevins, Yamana Gold
John Boal, CPP, PCI, CFE, University of Akron
Kevin Brear, MBCI, MEPS, MICPEM, Independent
Colin Brown, MA, PGC, De Beers Group
Hart Brown, Rent-A-Center
Michael Brzozowski, PSP, CPP, Symcor
Dirk Buerhaus, Fachkaufmann für Organisation, KOETTER GmbH & Co. KG Security
Donald Byrne, CBCP, CDCP, ISO Lead Auditor, GRCS, LLC
Jeffrey Campbell, CPP, Environmental Protection Agency
Chee-Seng Chan, CBCP, Certified Safety Officer, Certified Safety & BCM Auditor, Spot Management Services Pte Ltd
Gopal Choudhary, Wipro Limited, India
Daniel Colin, CPP, Hospira
Andrew Collins, CBCP/CBCA, Baylor Health Care System
Joseph Corry, CPP, Tennessee Valley Authority
Hugues Costes, ArcelorMittal
Georges Cowan, Business Continu-IT Partners
Gary Crowe, CRCMP, C.E.R.T., BCP, FEMA, ABA Mediation, Money Management International, Inc.
Eric Davoine, Independent
Robert Day, CPP, PCI, CSP, CRSP, CHRP, Grad IOSH, CPMSIA, Office of Regulatory Change Management
William Dill, Independent
Anthony DiSalvatore, CPP, PSP, PCI, REVEL
Larry Dodson, CPP, Cree, Inc.
Bobby Dominguez, CPP, CISSP, PMP, CRISC, GSLC, ITIL, PgMP, Infinite Computer Systems, Inc.
Jack Dowling, CPP, PSP, JD Security Consultants, LLC
Johan Du Plooy, CPP, TEMI Group
Herby Duverne, Taino Consulting Group

Eduard Emde, CPP, CISSP, BMKISS Europe
Thomas Engells, CPP, CPM, The University of Texas Medical Branch at Galveston Police Department
Dennis Ewart, Sobeys West
Ali Ferrer, PSP, Independent
Windom Fitzgerald, Fitzgerald Technology Group
Scott Fitzsimmons, Independent
Thomas Frank, CPP, AbbVie Inc.
Jeremiah Frazier, CPP, Coca-Cola
Nanpon Gambo, CSS, Nigerian Army
Mark Gaudette, CPP, CFI, LPC, Big Y Foods, Inc.
Douglas Goode, CPP, McRoberts Protective Agency
Robert Grieman, CPP, Securitas Security Services, USA, Inc.
Harold Grimsley, CPP, Blue Cross Blue Shield of Florida
Phillip Guffey, CPP, Roche
Steven Hather, Shadexi Consulting Pty Ltd
Donald Heitzman, CPP, Independent
Henri Hemery, Ph.D., RISK&CO
Derek Henderson, PSP, Haast Consulting Pty Ltd
Terry Higdon, CPTED Practitioner, NTS I, ABAT, ERMC
Wesley Holt, FMA, LEED BD&C, Electric Reliability Council of Texas
Christian Huenke, CHS-V, VPS, FedEx Trade Networks
William Imbrie, DynCorp International
Adam Incher, CPP, ACT Government, Shared Servcies
Christopher Jones, NBV Ltd
Bruce Kennedy, James Mintz Group
Graham Kerr, Hart Security Limited
Paul Kirvan, FBCI, CISA, Independent
Timothy Klass, CPP, Amazon Web Services
April Klukas, CPP, StandardAero
Dan Krefting, CHPA, Langara College
Joshua Kurjan, Independent
Misty Ladd, CPP, PCI, CPOI, Whelan Security
Billy Lamb, MBA, Praescient Analytics
Bill Lang, Independent
Robert Lang, CPP, CSO, CEM, Kennesaw State University
Russell Law, PSP, Gralion, LLC
James Leflar, Jr., CPP, CBCP, MBCI, Fleur de Lis Consultancy Group LLC
Jeffrey Leonard, CPP, PSP, Securitas Security Services, USA, Inc.
Denis Lynch, CPP, PSP, MBL Technologies
Anthony Macisco, CPP, The Densus Group
Tracy Male, CFCP, CBCA (DRII), Independent
Ronald Martin, CPP, Open Security Exchange
Scott Maxson, CPP, Independent
Joe Mazza, CHPP, Independent
Charles McBreen, CAMS, Members 1st F.C.U.
John McCaffery, Global Vision Consultancy
R. Paul McCauley, Independent
Allan McDougall, PCIP, CMAS, CISSP, CPP, Evolutionary Security Management
Mohamed Fadhel Meddeb, ISO 28000, Offline Solutions LLC
Gerald Mendes, Ieng FIEt CPP, GCL Services Limited
Alwin Miller, CPP, PSP, SAIC
Michael Miller, American Broadcasting Companies, Inc.
Stephen Miller, Eclipse Identity Recognition Corporation

Erin (Bear) Mitchell, Agility Recovery Solutions
William Moore, PSP, Jacobs Engineering Inc.
Richard Moore III, CISSP, CISM, GPEN, Citizens Bank
Eric Morse, CPP, Genentech
Joseph Nelson, CPP, State Street
Vick Nichols, ISO 28000 Lead Auditor, Independent
Mark Odom, Admiral Security
Michael O'Neil, NASPO
Philip Oppenheim, CBCP, Continuity Information Support Services
Jack Paul, PSP, Independent
Axel Petri, Deutsche Telekom AG
John Pettit, CPP, PSP, Independent
Rodney Pettus, The Jones Group
Andreas Poppius, Independent
Ren Powers, CISSP, City National Bank
William Prentice, Marine Security Initiatives, Inc.
Bala Ramanan, CBCI, CISM, CRISC, Microland Ltd
Malcolm Reid, CPP, CFE, CBCP, CORP, Brison Ltd
Ronald Ronacher, PSP, Arup
Brock Root, Luxottica Retail North America
Chris Rossis, Argonaut Security Ltd
Craig Rydalch, ISO 27001 Auditor, CISSP, PMP, CEH, GSNA, AIM Specialty Health
Zulfiqar Saleemi, Secure Options Group
Michael Sarni, CPP, Independent
James Saulnier, CPP, Sprint
Robert Schultheiss, CSC, Risk Decisions
Gordon Schwarzer, HiSolutions AG
Sarb Sembhi, Incoming Thought
Douglas Sinclair, SIT TAFE Ultimo
Avtar Singh, CPP, Independent
Jeffrey Slotnick, CPP, PSP, Setracon Inc.
Kevin Smith, CPP, Nationwide Insurance
Jose Miguel Sobron, United Nations
J. Kelly Stewart, NewCastle Consulting LLC
John Stewart, Luxottica
Ian Stilgoe, MCQI CQP, Independent
Bryan Strawser, Target Corporation
Timothy Sutton, CPP, Sorensen, Wilder and Associates
Jason Teliszczak, CPP, JT Environmental Consulting
Rajeev Thykatt, ISO 27001 Lead Auditor, BS 25999 Lead Auditor, Infosys BPO Ltd
Yoriko Tobishima, InterRisk Research Institute & Consulting, Inc.
Lina Tsakiris, CPP, TD Bank
Erika Voss, Microsoft
Doug Weeks, Hemlock Semiconductor
Jason Wells, Independent
Robert Wiest, CPP, Independent
Nick Wildgoose, Zurich Insurance Group
Pauline Williams-Banta, PMP, CRISC, MBCP, PMP, CRISC, MBCP, ITIL, The Energy Authority
Harold Wilson, CPP, Absolute Software Corporation
Paul Yung, Ph.D., Deloitte

Working Group Members

Working Group Chair: Marc H. Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative

Lyle Alexander, CPP, A.R.M Specialists Ltd
Paul Aube, CPP, Dessau
Dennis Blass, CPP, PSP, CFE, CISSP, CHSP, Children's of Alabama
John Boal, CPP, PCI, CFE, University of Akron
Dirk Buerhaus, Fachkaufmann für Organisation, KOETTER GmbH & Co. KG Security
Donald Byrne, CBCP, CDCP, ISO Lead Auditor, GRCS, LLC
Jeffrey Campbell, CPP, Environmental Protection Agency
Larry Dodson, CPP, Cree, Inc.
Johan Du Plooy, CPP, TEMI Group
Lisa DuBrock, CPA, CBCP, MBCI, RABQSA-RES, Radian Compliance, LLC
Thomas Frank, CPP, AbbVie, Inc.
Jeremiah Frazier, CPP, Coca-Cola
Bill Lang, Independent
James Leflar, Jr., CPP, CBCP, MBCI, Fleur de Lis Consultancy Group LLC
Denis Lynch, CPP, PSP, MBL Technologies
Anthony Macisco, CPP, The Densus Group
Eric Morse, CPP, Genentech
Philip Oppenheim, CBCP, Continuity Information Support Services
Bala Ramanan, CBCI, CISM, CRISC, Microland Ltd
Malcolm Reid, CPP, CFE, CBCP, CORP, Brison Ltd
Ronald Ronacher, PSP, Arup
Jeffrey Slotnick, CPP, PSP, Setracon Inc.
Timothy Sutton, CPP, Sorensen, Wilder and Associates
Jason Teliszczak, CPP, JT Environmental Consulting
Rajeev Thykatt, ISO 27001 Lead Auditor, BS 25999 Lead Auditor, Infosys BPO Ltd
Doug Weeks, Hemlock Semiconductor
Jason Wells, Independent

This page intentionally left blank.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

0 INTRODUCTION

0.1 General

This *Standard* provides guidance for management system audits for risk based disciplines of risk, resilience, security, crisis, continuity, and recovery management. The *Standard* uses an approach for auditing and conformity assessment consistent with the current versions of ISO 19011 *Guidelines for auditing management systems*, and ISO/IEC 17021 *Conformity assessment — Requirements for bodies providing audit and certification of management systems*.

The guidance in this *Standard* provides additional information for using the ISO 19011 and ISO/IEC 17021 standards for applications in evaluating risk and resilience based management systems addressing operational risks (including reputation). It describes establishing and managing an audit program as well as conducting individual audits. The competence of auditors is the foundation for conducting effective and credible audits; therefore, this *Standard* provides competence criteria for auditors conducting conformity assessment of a management system to a risk and resilience based management systems standard.

Auditors understand much of their activities involve interactions between people, therefore there is a need to build rapport, trust, and confidence while avoiding the creation of an adversarial atmosphere. An audit is a positive experience if the people being audited feel the audit adds value and may lead to opportunities for improvement. Good auditing techniques lead to a positive audit experience.

This *Standard* provides generic concepts of auditing a risk and resilience based management system. Organizations should adapt this guidance to fit the specific needs, size, nature and level of maturity of their risk and resilience based management system. This *Standard* can be used by anybody involved in the conformity assessment of a risk and resilience based management system.

0.2 Risk and Resilience Based Management System Audits

A management system audit determines if the organization is conforming to the relevant requirements, including standards, regulations, contracts, policies, procedures, controls, and specifications. A management system audit is a documented process to impartially collect, examine, and evaluate pertinent evidence. The process determines if all the elements of a management system standard have been developed, documented, implemented, and tested in accordance with defined requirements and are effectively meeting their prescribed objectives. An audit should provide the management of an organization unbiased empirically-based information necessary to:

a) Determine effectiveness of the management system, its elements, and how the management system supports the objectives of the organization;

b) Identify inefficiencies, deficiencies, and weaknesses in the management system;

c) Provide awareness of actual and potential risks;

d) Assess training effectiveness;

e) Promote risk and resilience awareness;

f) Evaluate and communicate practices relative to accepted industry practices; and

g) Identify opportunities for improvement.

The audit should assess conformance to the management system by determining if and how it is adhering to the requirements as articulated in the organization's policies, procedures, task specifications, and/or work instructions. A management system audit is not simply a checklist of evidence of the existence of elements of the management system. The audit confirms that the organization is indeed doing what it says by evaluating the effectiveness, efficiency, performance, and intended outcomes of its implementation of the management system. An auditor should have the necessary and relevant professional knowledge, skills, and qualifications relative to the specific standard being audited as well as types of risks and organization being audited. Therefore, to conduct an audit the auditor should understand:

a) The requirements of the relevant standard(s);

b) Principles of a risk and resilience based management systems approach and auditing;

c) Legal and other requirements applicable to the organization and its operations;

d) Risk from a business, operational, and organizational perspective;

e) Industry and business specific information pertinent to the organization; and

f) Concepts of risk and resilience based management.

In determining the conformance to the management system standard, the auditor will verify if the requirements of the standard are being properly implemented by the management system. An effective audit is non-adversarial and conducted from the perspective of assessing what the organization is doing effectively and identifying opportunities for improvement. The audit should add value to the organization by identifying areas where management system elements are not being effectively implemented and providing an understanding of the reasons why. The auditor collects objective evidence to establish whether conformance is achieved. The audit evaluates if the process and the individual activities are effective, and provides a basis to identify opportunities to improve the effectiveness and efficiency.

0.3 Audits versus Inspections

As defined in the ISO 17000:2006 *Conformity assessment – Vocabulary and general principles* an audit is:

> *A systematic, independent, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled. NOTE: Whilst "audit" applies to management systems, "assessment" applies to conformity assessment bodies as well as more generally.*

An inspection is defined as:

> *An examination of a product design, product, process or installation and determination of its conformity with specific requirements or, on the basis of professional judgement, with general requirements. NOTE: Inspection of a process may include inspection of persons, facilities, technology and methodology.*

Table 1: Differences between audits and inspections.

Audits	Inspections
• Systematic, independent, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled. (Source: ISO 17000:2004)	• Examination of a product design, product, process or installation and determination of its conformity with specific requirements or, on the basis of professional judgment, with general requirements. (Source: ISO 17000:2004)
• Evaluates fulfillment of requirements and effectiveness of a management system. • Determine whether systems are in place and working effectively. • Compare physical and operational conditions with systems and standards. • Follow a pattern and interrelationships between elements of the standards.	• Determination conformity of a product, process or service with specific requirements. • Examine extent of physical or operational conformance to set standards. • Generally do not consider systems issues or only in limited scope.
• Evaluate the effectiveness of risk treatments based on risk assessment and objectives of the organization.	• Can identify risks.
• Document areas of non-conformance and identify opportunities for improvement. • Involve management team, decision-making, and human-technology interface.	• Record as-inspected condition. • Report non-conformances for corrective action.
• Time cycles linked to business management cycles.	• Time cycle not linked to the management and fiscal cycle of the organization but rather product, process or service requirements.
• Generally takes days to conduct.	• Generally take hours to conduct.

0.4 Types of Management System Audits

Depending on the relationships between participants, an audit usually takes one of two forms:

a) Internal or first-party audit; and
b) External - or second or third-party audit.

0.4.1 First-party Audits

Auditors working on behalf of the organization, either its own auditors or subcontracted auditors, conduct first-party audits. A company auditing a sister company is also considered a first-party audit if they belong to the same parent company. The organization is evaluating its conformance and the effectiveness of the management system standard to an adopted external standard and/or

requirements mandated by the organization. When conducting internal audits, care should be taken to ensure the independence of the auditors and avoid conflicts of interest. This can be accomplished through a separate internal group tasked with auditing or by outsourcing the audit activities to an external auditing organization. In either case, auditors should be well trained and able to maintain objectivity and impartiality. Internal auditors should not audit their own work. By assigning individual owners for sections of the management system, a conflict of interest can be avoided by having auditors review sections they do not own. Some internal auditors can emphasize identifying root causes of strengths and weakness of the management system to identify accepted industry practices and opportunities for improvement.

0.4.2 Second-party Audits

Second-party audits are conducted by an external party within a contractual relationship. Second-party audits are typically customer or supplier audits and are often necessary to assess risks in a supply chain process. Second-party audits are usually more formal than first-party audits given that they are conducted within an existing or potential contractual relationship. It is important to understand the relationship between the parties of the audit to ensure that it is being conducted in an unbiased fashion, as well as to identify areas of potential bias. Second-party audits may focus on specific elements of the management system standard most relevant to the terms of the contract.

0.4.3 Third-party Audits

Third-party audits are conducted by an independent external organization which does not have a business interest in the organization being audited. Third-party audits are free of conflicts of interest associated with customer and supplier relationships and audits conducted by auditors working on behalf of the organization. Third-party audits provide the basis for conformity assessments for certification to a standard by a certification body or registrar. Government agencies working with regulated industries also use them for regulatory compliance assessments. Third-party audits may also be performed on one organization on behalf of another organization. In such cases, the relationship between the organizations should be clearly defined. Third-party audits are particularly useful if an organization is subject to multiple second-party audits, or if action is lacking from first-party audits to correct non-conformances and opportunities for improvement.

0.5 Conformity Assessment and Certification

As defined in the in the ISO 17000:2006 *Conformity assessment – Vocabulary and general principles* a conformity assessment is:

> *Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled.*

There are three types of conformity assessment:

a) First party - carried out by the organization itself, or by someone working on behalf of the organization. It is a self-assessment and self-declaration;

b) Second party - performed by person or organization that has a user interest in the organization being audited; and

c) Third party - performed by a body that is independent of the organization that provides the product/services and is not a user of the product/services. An independent certification body certifies that another organization complies with the standard and issues it with a certificate to this effect.

Certification of a management system ("certification") is a third-party conformity assessment activity. Bodies performing this activity are therefore third-party conformity assessment bodies ("certification body").

NOTE 1: Certification of a management system is sometimes also called "registration", and certification bodies are sometimes called "registrars."

NOTE 2: A certification body can be non-governmental or governmental (with or without regulatory authority).

Conformity assessment and certification to a relevant management system standard is a means of providing assurance that an organization of any type has implemented a system for the management of risk and resilience in line with the standard, as well as the organization's policy and procedures. The conformity assessment references of this *Standard* are sector specific guidance based on the ISO/IEC 17021:2011 and provides additional recommendations for conformity assessment in those areas which are deemed necessary and relate specifically to risk and resilience management.

The conformity assessment references of this *Standard* have been specifically developed to assist in the certification of risk and resilience based management systems that fulfil the requirements of ANSI/ASIS SPC.1-2009 *Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use*. The contents of this *Standard* may also be used to support certification of resilience, security, crisis, and business continuity management systems that are based on other or additional sets of specified requirements.

The conformity assessment references of this *Standard* are intended for use by bodies that carry out audit, conformity assessment, and certification of risk and resilience based management systems. It gives generic recommendations for such certification bodies performing audit, conformity assessment, and certification of organizations' management systems. Such bodies are referred to as "certification bodies" or "registrars."

Certification activities involve the audit of an organization's management system. The form of attestation of conformity of an organization's management system to the management system standard or other specified requirements is normally a certification document or a certificate.

The organization being certified develops its own management systems tailored to its needs and resources and, other than where relevant legal requirements specify to the contrary, it is for the organization to decide how the various components of the management system will be arranged. The degree of integration between various management system components will vary from organization to organization. It is therefore appropriate for certification bodies that operate in accordance with the assessment references of this *Standard* to take into account the culture and

practices of their clients with respect to the integration of their management systems within the wider organization.

Auditing Management Systems: Risk, Resilience, Security, and Continuity—Guidance for Application

1 SCOPE

This *Standard*:

a) Is a sector specific standard based on the ISO 19011: 2011 and ISO/IEC 17021:2011;

b) Provides guidance for conducting conformity assessment of the ANSI/ASIS SPC.1-2009 *Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use* standard, as well as similar risk and resilience based management system standards (e.g., ISO 22301:2012, *Societal security - Business continuity management systems – Requirements*; ANSI/ASIS/BSI BCM.01-2010, *Business Continuity Management Standard*; ISO 28000:2007, *Specification for security management systems for the supply chain*; ASIS/ANSI PAP.1-2012, *Security Management Standard: Physical Asset Protection*; etc.);

c) Provides guidance on auditing risk and resilience based management system standards for the disciplines of risk, resilience, security, crisis, continuity, and recovery management, including principles of auditing, managing the audit program, and conducting audits, as well as evaluation of competence of persons involved in the audit process;

d) Describes the process of attestation of fulfillment of the requirements of a risk and resilience based management system standard for the disciplines of risk, resilience, security, crisis, continuity, and recovery management;

e) Provides guidance on the management of audit programs, conduct of internal or external audits of the management system and risk, resilience, security, crisis, continuity, and recovery management, as well as on competence and evaluation of auditors;

f) Provides guidance for bodies providing auditing and third party certification of risk and resilience based management system standards for the disciplines of risk, resilience, security, crisis, continuity, and recovery management; and

g) Provides confidence and information to stakeholders that the requirements of standards for risk, resilience, security, crisis, continuity, and recovery management are being met.

Organizations, of all types and sizes can use the concepts and guidance of this *Standard*. It is recommended that organizations implementing risk and resilience based management system standards use the procedures described in this *Standard* in conjunction with the ISO 19011:2011 to conduct their internal audit activities.