****

**Table of Contents**

[IS Audit/Assurance Program for Cybersecurity: Based on the NIST Cybersecurity Framework Audit Program 3](#_Toc469560728)

[Audit Subject: Cybersecurity: Based on the NIST Cybersecurity Framework Audit Program 3](#_Toc469560729)

[Audit Objectives 3](#_Toc469560730)

[Audit Scope 3](#_Toc469560731)

[Business Impact and Risk 3](#_Toc469560732)

[Minimum Audit Skills 4](#_Toc469560733)

[Testing Steps 4](#_Toc469560734)

**Note:** The cybersecurity audit program worksheet is provided as a separate file.

# IS Audit/Assurance Program for Cybersecurity: Based on the NIST Cybersecurity Framework Audit Program

## Audit Subject: Cybersecurity: Based on the NIST Cybersecurity Framework Audit Program

In light of the increasing volume and sophistication of cyberattacks, ISACA has developed an audit/assurance program based on the NIST Cybersecurity Framework to provide organizations with a formal, repeatable way to evaluate cybersecurity controls.

The objective of a cybersecurity audit is to provide management with an evaluation of the effectiveness of cybersecurity processes, policies, procedures, governance and other controls. The review will focus on cybersecurity standards, guidelines and procedures as well as the implementation of these controls. The audit/assurance review will rely upon other operational audits of the incident management process, configuration management and security of networks and servers, security management and awareness, business continuity management, information security management, governance and management practices of both IT and the business units, and relationships with third parties.

The primary security and control issues include:

* Protection of sensitive data and intellectual property
* Protection of networks to which multiple information resources are connected
* Responsibility and accountability for the device and information contained on it

## Audit Objectives

* Provide management with an assessment of their cybersecurity policies and procedures and their operating effectiveness.
* Identify security control concerns that could affect the reliability, accuracy and security of the enterprise data due to weaknesses in security controls.
* Evaluate the effectiveness of response and recovery programs.

## Audit Scope

The audit/assurance program is built on the following five critical cybersecurity activities:

* Identify
* Protect
* Detect
* Respond
* Recover

The auditor conducting the audit will identify the scope of organizational systems and assets to be reviewed. The audit/assurance program can be adapted to support various business processes, applications or systems with different security requirements.

## Business Impact and Risk

Cyberincidents can have a financial, operational, legal and reputational impact. An organization’s role in critical infrastructure can also increase the potential impact of a cyberincident. Some examples of impact from a cyberincident may include:

* Negative publicity resulting in loss of reputation
* Loss of intellectual property or trade secrets
* Fines, lawsuits and legal fees resulting from noncompliance or loss of confidential or consumer information
* Forensic investigation costs
* Public relations campaign costs to improve public image
* Technology improvement costs to mitigate and improve cybersecurity controls
* Loss of time and productivity

## Minimum Audit Skills

The IT audit and assurance professional must have an understanding of security and controls. Because this is a dynamic field, professionals performing this audit should ensure that they have performed the necessary research to understand the underlying technologies used in cybersecurity to identify, protect, detect and respond to cyberthreats and attacks. However, it is important that the auditor has sufficient functional and business knowledge to assess alignment with the business strategy. Professionals holding the CISA certification should comply with ITAF standard 1006 Proficiency.

## Testing Steps

Audit steps have been developed for each NIST Cybersecurity Framework subcategory to evaluate the effectiveness of the organization’s controls. Refer to the Cybersecurity NIST Audit Program Excel spreadsheet for the full audit/assurance program.

**ISACA®**

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity NexusTM (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

**Disclaimer**

ISACA has designed and created *IS Audit/Assurance Program Cybersecurity: Based on the NIST Cybersecurity Framework* (the “Work”) primarily as an educational resource for audit professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, audit professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

**Reservation of Rights**

©2016 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

**ISACA**

3701 Algonquin Road, Suite 1010

Rolling Meadows, IL 60008 USA

Phone: +1.847.253.1545

Fax: +1.847.253.1443

Email: *info@isaca.org*

Website: *www.isaca.org*

Provide feedback: *www.isaca.org/auditprograms*

Participate in the ISACA Knowledge Center: *www.isaca.org/knowledge-center*

Follow ISACA on Twitter: *https://twitter.com/ISACANews*

Join ISACA on LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*

Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

ISBN 978-1-60420-589-3

**Acknowledgments**

**Lead Developers**

Russ Horn, CISA, CRISC, CISSP, CoNetrix, USA

Stephanie Chaumont, CISA, CISSP, Security+, CoNetrix, USA

Ed McMurray, CISA, CISSP, CTGA, CoNetrix, USA

**Expert Reviewers**

Ian Cooke, CISA, CRISC, CGEIT, COBIT 5 Implementer & Assessor, CFE, CPTS, DipFM, ITIL Foundation, Six Sigma Green Belt, An Post, Ireland

Sue Rusher, CISA, CRISC, CIA, CFE, CISSP, BlueCross BlueShield of South Carolina, USA

Peter Tessin, CISA, CRISC, MSA, PMP, ISACA, USA

**Board of Directors**

Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Chair

Theresa Grafenstine, CISA, CGEIT, CRISC, CIA, CGAP, CGMA, CPA, U.S. House of Representatives, USA, Vice-chair

Robert Clyde, CISM, Clyde Consulting LLC, USA, Director

Leonard Ong, CISA, CISM, CGEIT, CRISC, CPP, CFE, PMP, CIPM, CIPT, CISSP ISSMP-ISSAP, CSSLP, CITBCM, GCIA, GCIH, GSNA, GCFA, Merck, Singapore, Director

Andre Pitkowski, CGEIT, CRISC, OCTAVE, CRMA, ISO27kLA, ISO31kLA, APIT Consultoria de Informatica Ltd., Brazil, Director

Eddie Schwartz, CISA, CISM, CISSP-ISSEP, PMP, WhiteOps, USA, Director

Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, FACS CP, BRM Holdich, Australia, Director

Tichaona Zororo, CISA, CISM, CGEIT, CRISC, CIA, CRMA, EGIT | Enterprise Governance (Pty) Ltd., South Africa, Director

Zubin Chagpar, CISA, CISM, PMP, Amazon Web Services, UK, Director

Rajaramiyer Venketaramani Raghu, CISA, CRISC, Versatilist Consulting India Pvt. Ltd., India, Director

Jeff Spivey, CRISC, CPP, Security Risk Management, Inc., USA, Director

Robert E Stroud, CGEIT, CRISC, Forrester Research, USA, Past Chair

Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past Chair

Greg Grocholski, CISA, SABIC, Saudi Arabia, Past Chair

Matt Loeb, CGEIT, FASAE, CAE, ISACA, USA, Director