**Name of Organization**

**Consolidated List of Standards**

December 2021

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

The (Name of Organization) Consolidated List of Standards document is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute this document to individuals on a need-to-know basis. Distribution by other individuals without prior authorization is prohibited. This document is unclassified but contains sensitive information.

# Introduction and Purpose

The (Name of Organization) Consolidated List of Standards document establishes a formal set of standards that are used to create Security Incident Response Plans, Teams and Processes to address Cyber Security Incidents.

# Incident Response Standards

### [Federal Emergency Management Agency (FEMA) National Frameworks](https://www.fema.gov/emergency-managers/national-preparedness/frameworks)

### [National Incident Management System (NIMS)](https://www.fema.gov/emergency-managers/nims)

### [ISO/IEC 27035:2011: Information Security Incident Management](http://www.iso.org/iso/catalogue_detail?csnumber=44379)

### [SANS: Creating and Managing an Incident Response Team](https://www.sans.org/reading-room/whitepapers/incident/creating-managing-incident-response-team-large-company-1821)

### [CERT: Handbook for Computer Security Incident Response Teams (CSIRTs)](https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305)

### [NIST SP 800-61: Computer Security Incident Handling Guide](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)

### [ISACA: Incident Management and Response](http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Incident-Management-and-Response.aspx)

# Incident Management Maturity Standards

[SIM3: Security Incident Management Maturity Model](https://www.trusted-introducer.org/SIM3-Reference-Model.pdf)

### [CERT: Incident Management Capability Metrics (IMCM)](https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=295919)

### [CERT: An Introduction to the Mission Risk Diagnostic for Incident Management Capabilities (MRD-IMC)](https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=91452)

### [Threat Hunting Maturity Model](https://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html)