Section 1

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Number** | **Standardisation body** | **Title of standard** | **Status** | **DF area of focus** | **Three‐sentence‐max description of standard** | **Similar ISO standard(s)** | **Downloadable link** |
| 1 | MIRE | CybOX, Cyber Observable eXpression |  | Evidence collection and communication | The standard is a schema for the specification, capture, characterization and communication of properties in an oprerational domain. | ISO/IEC 27037: Information security incident management | http://cybox.mitre.org/ |
| 2 | MIRE | MAEC, Malware Attribute Enumeration and Characterization A standardized language for Attribute-based Malware Characterization |  | The standard is focused confidentiality with regards to malware and their behaviour. | It is a standardized language for encoding and communicatinh high-fifelity informstion about malware based upon attributes such as behaviours, artifacts and attack patters. | ISO/IEC 27037: Information security incident management | http://maec.mitre.org/index.html |
| 3 | IETF | IODEF, The Incident Object Description Exchange Format |  | The standard focuses on incident planning and repsonse in teams. | The Incident Object Description Exchange Format (IODEF) defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents. | ISO/IEC 27035: Information security incident, Part 3  Management | http://tools.ietf.org/html/rfc5070 |
| 4 | IETF | MILE, Digital Forensics Extension for IODEF |  | The standard focuses on sharing digital forensic information between various organizations | The goal is to allow a tool independent format to share information between organizations focused on digital forensics: drive images, file carving, metadata, and related hashes. As with IODEF and its extensions, it is defined using XML. | ISO/IEC 27035: Information security incident, Part 2  Management | http://tools.ietf.org/html/draft-inacio-mile-forensics-00 |
| 5 | NIST | Guidelines on Mobile Device Forensics |  | Deigital Forensics in mobile devices | The guide is concerned with performing digital forensics on mobile devices using accepted methods. | ISO/IEC 27035: Information security incident, Part 2  Management | http://csrc.nist.gov/publications/PubsSPs.html#800-101 |
| 6 | NIST | *Guide to Cyber Threat Information* Sharing |  | Iincident planning and repsonse in teams. | The focus is to assist organizations in establishing, participating in, and maintaining information sharing relationships throughout the incident response life cycle | ISO/IEC 27035: Information security incident, Part 2  Management | http://csrc.nist.gov/publications/drafts/800-150/sp800\_150\_draft.pdf |
| 7 | NIST | *NIST SP 800-61r2:*Computer Security Incident Handling Guide |  | Iincident planning and repsonse in teams. | The focus of the publication is assist organizations in establishing comp  uter security incident response capabilities and handling  incidents efficiently and effectively.. | ISO/IEC 27035: Information security incident, Part 2  Management | http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf |
| 8 | NIST | NIST SP.800-37: Guide to Integrating ForensicTechniques into Incident Response |  | Iincident planning and repsonse in teams. | This publication is intended to help organizations in investigating computer security incidents andtroubleshooting someinformation technology (IT) operational problems by providing practical guidanceon performing computer and network forensics | ISO/IEC 27035: Information security incident, Part 2  Management | http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf |

Section 2

ISO/IEC 27001 vs. NIST SP.800-37

The Information Security Management System of ISO 27001 standard is a management standard for which compliance requires the the organization to have a suite of management controls in place.

NIST Risk Management Framework is focused on defining,assessing, implementing, and monitoring the risk of a specific system.

ISO/IEC 27037 vs. CybOX

ISO/IEC 27037 and CybOX both provide guidelines for evidence (data) specification, capturing and acquisition in an operational domain.

The difference is however, that the guidelines for ISO/IEC 27037 extend towards preservation of that collected evidence.

ISO/IEC 27035 Part 2 vs. NIST SP.800-61r2

ISO/IEC 27035 Part 2 and NIST SP.800-61r2 are both concerned with effectivly establishing the planning and preparations for responding to incidents within the context of Digital Forensics and Computer Security.

ISO/IEC 27035 Part 3 vs. IETF:IODEF

ISO/IEC 27035 Part 3 and IETF IODEF both have an element of reporting efficiently to a information security incident that may have occurred.

The difference is however that IETF:IODEF is limited to reporting, like sending an incident report to the Computer Security Incident Response Teams (CSIRTs), whilst ISO/IEC 27035 Part 3 has a more comprehensive scope which includes Detection, Reporting, Assessment, Decision and Response to incidences that may have occurred.