**OpenVuln Security Framework Tool**

**Abstract**

Our objective is to design a Security Framework for Kumaraguru College of Technology which will be further modified for enterprise use.

**Literature Review**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Paper / Title | Author | Year | Journal | Abstract | Proposed Technique | Limitations/  Improvements |
| NIST Cybersecurity Framework | National Institute of Standards and Technology | 2018 | National Institute of Standards and Technology | The NIST Cybersecurity Framework aims to provide a “prioritized, flexible, repeatable, and cost-effective approach” to cybersecurity risk management. | * Identify * Protect * Detect * Respond * Recover | * CSF does not make NIST SP 800-53 easier * Store log data for only 30 days * Only on-premises, No Clear definition for Cloud Security * RBAC – “Role-Based Access Control” not suitable for cloud-based infrastructure |
| Protecting Controlled Unclassified Information in Non-federal Systems  and Organizations | Ron Ross  Patrick Viscuso  Gary Guissanie  Kelley Dempsey  Mark Riddle | 2016 | National Institute of Standards and Technology | The protection of Controlled Unclassified Information (CUI) resident in non-federal systems and organizations is of paramount importance to federal agencies. The federal agencies with recommended security requirements for protecting the confidentiality of CUI. The requirements are intended for use by federal agencies in contractual vehicles or other agreements. | * Identity Management, Authentication and Access Control * Awareness and Training * Backups of information are conducted, maintained, and tested * Data is destroyed according to policy * Policy and regulations regarding the physical operating environment for organizational assets are met * Protection processes are improved |  |
| IT Governance and Information Security – Guides, Standards and Frameworks | Yassine Maleh  Mamoun Alazab  Mustapha Belaissaoui | 2022 | Book published by CRC Press | Discusses strategic information technology governance and information security: guides, practices, and maturity frameworks | Highlights ISO standards, IT Service Management (ITSM) frameworks such as ITILv4, IT Asset Management (ITAM), IT Security Management |  |
| Cybersecurity Frameworks  Comparing, Contrasting and Mapping | Matthew Hudnall, The University of Alabama | 2019 | IEEE Computer Society | Three current cybersecurity professional and academic  program schemes target cyber education, training,  and workforce roles. They have complementary  elements that can serve as a pathway from learning  cyber to working cyber if correctly navigated. —discusses the NICE 2.0, NSA CAE-CD, CSEC2017 cybersecurity frameworks | Discusses the NICE (National Initiative on Cybersecurity Education) 2.0, NSA CAE-CD(Centers of Academic Excellence in Cyber Defense Education), CSEC2017 (Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity) cybersecurity frameworks | This paper goes in details about the frameworks proposed by the standard regulatory bodies such as NIST (National Institute of Standards and Technology), NSA (National Security Agency) and Centers of Academic Excellence in  Cyber Defense Education (CAE-CD) boldly stating these frameworks as curricular foundations for cybersecurity without referencing the other ISO standards proposed for cybersecurity such as ISO/IEC 27002, ISO/IEC 27031, ISO/IEC 27032 etc. |
| National Initiative for Cybersecurity  Education (NICE)  Cybersecurity Workforce Framework | Rodney Petersen Danielle Santos; Karen A. Wetzel Matthew C. Smith  Greg Witte | November 2020 | NIST Special Publication 800-181 | Describes the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), a reference structure that describes the interdisciplinary nature of the cybersecurity work. It serves as a fundamental reference resource for describing and sharing information about cybersecurity work and the knowledge, skills, and abilities (KSAs) needed to complete tasks that can strengthen the cybersecurity posture of an organization. | Uses the NICE Cybersecurity Workforce Framework), as a reference that describes the interdisciplinary nature of the cybersecurity work. | This framework proposes tasks , roles and drafts strategies for cybersecurity workforce and employees in the field of cybersecurity but it doesn't incorporate strategies and methods for maintaining and managing assets that hold sensitive and confidential data where other frameworks do. |
| The challenges of cybersecurity frameworks to protect data required for the  development of advanced maintenance | Jaime Campos  Pankaj Sharma Erkki Jantunen  David Baglee  Luca Fumagalli | 2016 | Open access article published by Elsevier B.V | Highlight the important aspects of the data management in condition monitoring and maintenance, especially when the emergent technologies, such as the cloud computing and big data, are to be considered in the maintenance department. In addition, one of the main data management elements highlighted in the current work are the cybersecurity issues which might be one of the biggest obstacles hindering the development of cloud based big data for condition-based maintenance (CBM) purposes. | References the cloud computing framework proposed by NIST and other frameworks proposed by Cloud Security Alliance (CSA). | This paper puts forth a lot of reasons to why people hesitate to store their confidential and sensitive data in the cloud servers and the risk associated with it while talking about the advantages associated with the cloud.  While it highlights the benefits and disadvantages of cloud computing and data storage and maintenance in it, it completely leaves out the theoritical principles, strategies, methods and countermeasures in various aspects of cybersecurity. |

**Reference:**