**A Comparative Study of Cyber Security Standards/Framwork.**

**Dr. Sanjay Shinde**, IPS, Research Scholar, VAMNICOM, Pune, [deosanja](mailto:deosanjay64@gmail.com)[y64@gmail.com](mailto:y64@gmail.com)

**Dr.Yashwant Patil**, Research Guide, VAMNICOM, Pune, yspatil@vamnicom.gov.in

# Abstract:

Cyber security is the practice of protecting and recovering computer systems, networks, devices and programs from any type of cyber attack.The world is increasingly reliant on technology and will continue to increase due to its evolving nature. Therefore, the cyber security importance is on the rise. The cyber security standards are therefore assume immense importance to improve the security of information technology systems, networks and critical infrastructure.[1] The cyber security standard defines both functional and assurance requirements within a product, system, process.[2]

The various Cyber Security standards and Cyber Security frameworksare in use and applicable for all type of organizations. The major cyber security standards used in banking sector are International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Payment Card Industry Data Security Standard (PCI DSS), Reserve Bank of India Framework (ReBIT) etc.

In the year 2017, RBI has recommendedcyber security framework for banks in India to ensure adequate cyber-security preparedness among banks on a continuous basis.[3] The security framework area includes IT Governance, Information Security, IS Audit, IT Operations, IT Services Outsourcing, Cyber Fraud, Business Continuity Planning, Customer Awareness programs and Legal aspects.In spite of these security standards the cyber security issues have increased. In order to study the various features and its applications for available cyber security standards the present paper provides an overview of various cyber security standards and its comparison on important parameters. The researcher has made an attempt to review the existing cyber security standards and its applicability.

# Key Words:

Cyber Security Standards, Cyber Security Frameworks, Banking Frauds. Reserve Bank of India. Information Technology.

# Cyber Security Standards

Cyber security standards enhance security and contribute to risk management in several important ways. Standards help establish common security requirements and the capabilities needed for secure solutions.[4] Security standards facilitate sharing of knowledge and best practices by helping to ensure common understanding of concepts, terms and definitions, which prevents errors.

The standards consist of basic rules that the organization is supposed to follow in order to maintain compliance with any of the cybersecurity standards.[5] Many of the Financial Institutions/Banks are utilizing different standards for the extension of security***.*** The cyber security standards used in many of the countries are to protect themselves and their customers from hackers/fraudsters.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**1. Julian Jang-Jaccard, Surya Nepal, A survey of emerging threats in cybersecurity,**

**Journal of Computer and System Sciences, Volume 80, Issue 5, 2014, Pages 973-993, ISSN 0022-0000,** [**https://doi.org/10.1016/j.jcss.2014.02.005**](https://doi.org/10.1016/j.jcss.2014.02.005)**.**

**2.Wiley Handbook of Science and Technology for Homeland Security Date Published: 2009 by Karen Scarfone (NIST), Dan Benigni (NIST), Tim Grance (NIST)**

**3. RBI Letter Ref No. RBI/2015-16/418 DBS.CO/CSITE/BC.11/33.01.001/2015-16, Dated June 2, 2016, To The Chairman/ Managing Director /Chief ExecutiveOfficer All Scheduled Commercial Banks (excluding Regional Rural Banks), https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=1721**

**4. Cyber Security Standards Karen Scarfone, Dan Benigni and Tim Grance National Institute of Standards and Technology (NIST), Gaithersburg, Maryland,**

[**https://tsapps.nist.gov/publication/get\_pdf.cfm?pub\_id=152153#:~:text=Cyber%20security%20standards%20enhance%20security,capabilities%20needed%20for%20secure%20solutions**](https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152153#:~:text=Cyber%20security%20standards%20enhance%20security,capabilities%20needed%20for%20secure%20solutions)**.**

**5.** [**https://www.educba.com/cyber-security-standards/**](https://www.educba.com/cyber-security-standards/)

In India there are different sectors of Banks viz. Public Sector Banks, Private Sector Banks and Cooperative Sector Banks. These all types of banks are regulated by Reserve Bank of India, for controlling and monitoring many of the aspects, including cyber security. Globally there are many Cyber Security Standards, which have been suggested to use for secure Banking. In India, RBI has suggested Cyber Security Framework.

The research paper is focused on existing cyber security standards and their framework. All the financial sectors are utilizing different standards or mixed type of standards viz. International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Payment Card Industry Data Security Standard (PCI DSS) which specifies the security standards for handling credit card information, Health Insurance Portability and Accountability (HIPAA) is used for formation of national standards to protect patient health information, British Standards, Reserve Bank of India Framework (ReBIT), [Centerfor Internet Security](https://www.cisecurity.org/) (CIS), COBIT (Control Objectives for Information) Currently no standard ensures 100% protection from Cyber Crimes happenings in finance/Banking sector. The RBI’s Framework is in practice since 2017 and it is also not able to control the recent incidents ofcyber crimesas expected. The Research paper titled **“A Comparative Study of Cyber Security Standards”** is an attempt tocompare various standards, frameworks, and suggest improvements/value additions to Cyber Security Frameworkof the RBI.

# OBJECTIVES OF THE STUDY

The present study is carried out with following objectives:

* 1. To study various Cyber Security Standards and Cyber Security frameworks applicable to banking sector
  2. To compare and analyze features and applications of various cyber security standards

# RESEARCH METHODOLOGY ADOPTED

The present study is undertaken with analysis of secondary data from available sources i.e. Books, Journals, magazines, websites, RBI portal, other member bank’s of Banks portals, Cyber Crime cell of Police Department in PCMC area, Government of Maharashtra, India etc.

# PREVAILING CYBERSECURITY STANDARDS

The principal objective of [Cybersecurity](https://en.wikipedia.org/wiki/Cybersecurity) standards is to reduce the risks, including preventing or mitigating [cyber-attacks](https://en.wikipedia.org/wiki/Cyber-attack), which includes tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies. Cybersecurity standards have existed over several decades and many of the revisions have happened.[6] Although there are many of the standard’s available worldwide, the researchers hasundertaken comparative study of selected standards. Below are the various cyber security standards.

1. International Organization for Standardization (ISO/IEC 27001)
2. Payment Card Industry Data Security Standard (PCI DSS)
3. National Institute of Standards and Technology (NIST)
4. General Data Protection Regulation (GDPR)
5. Reserve Bank of India Framework (ReBIT)
6. COBIT (Control Objectives for Information and Related Technologies)
7. BSI (British Standards Institution) Standards
8. [Center for Internet Security](https://www.cisecurity.org/) (CIS) Framework
9. Secure Controls Framework (SCF)

Most of the Standards listed are based on the parameters given below:

* Level of Preparedness
* Unidentified Devices on Internal
* Intrusion Attempts
* Security Incidents
* Mean Time to Detect (MTTD)
* Mean Time to Resolve (MTTR)
* Mean Time to Contain (MTTC)
* First Party Security Ratings
* Average Vendor Security Rating
* Patching Cadence
* Access Management Company vs Peer Performance
* Vendor Patching Cadence
* Mean Time for Vendors Incidence

The cyber security controls vary in the various Cyber Security Standards.

# CYBERSECURITY STANDARDS- TERMS OF REFERENCES

**Cybersecurity Standard:** A cybersecurity standard is a formal set of guidelines, requirements, and best practices developed and published by recognized standardization bodies or organizations.[7] These standards are usually created through a consensus-based process involving experts from various industries and sectors. They provide specific and detailed instructions on how to implement security controls and measures to protect information, systems, and networks.

**Cybersecurity Framework:** A cybersecurity framework is a more flexible and high-level approach to cybersecurity. It is typically a set of guidelines, best practices, and principles that help organizations asses and manage their cybersecurity risks, identify gaps in their security posture, and prioritize areas for improvement. Frameworks are often developed by government agencies, industry organizations, or public-private partnerships.

A popular cybersecurity framework is the NIST Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST) in the United States. It consists of five functions: Identify, Protect, Detect, Respond, and Recover, which provides a structure for organizations to manage and improve their cybersecurity capabilities.[8]

The researcher has shortlistedthe available standard on Cyber Security and has made comparative analysis of the various standards to assess the conveys of flame standards and domain wise controls defined.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**6.** [**https://en.wikipedia.org/wiki/IT\_security\_standards**](https://en.wikipedia.org/wiki/IT_security_standards)

**7.** [**https://www.itgovernanceusa.com/cybersecurity-standards#:~:text=A%20cybersecurity%20standard%20is%20a,and%20data%20from%20cyber%20threats**](https://www.itgovernanceusa.com/cybersecurity-standards#:~:text=A%20cybersecurity%20standard%20is%20a,and%20data%20from%20cyber%20threats)**.**

**8.** [**https://www.nist.gov/cyberframework/online-learning/five-functions**](https://www.nist.gov/cyberframework/online-learning/five-functions)

**1. ISO/IEC 27001 (International Organization for Standardization):**

The international standard developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This standard provides a systematic approach for managing and protecting information assets within organization.[9] The standard emphasizes in the implementation of an Information Security Management System (ISMS) and includes comprehensive controls across various domains. The standard is globally recognized and widely adopted as a benchmark for information security management.[10] The highly features of the standards are:

**Focus:** Information security management system (ISMS)

**Scope:** Applies to any organization, regardless of its size or sector

**Key Features:** Risk assessment and management, controls implementation, continual improvement

**Compliance:** Organizations can undergo an audit to achieve ISO/IEC 27001 certification

**2. PCI DSS (Payment Card Industry Data Security Standard):**

This standard is applicable for payment cards and is developed by the Payment Card Industry Security Standards Council (PCI SSC) to protect cardholder data and secure payment card transactions.[11] This standard consists of a set of requirements that organizations handling payment card information must comply with. This standard is primarily applicable to organizations involved in payment card processing, such as merchants, financial institutions, and service providers. The highly features are:

**Focus:** Protecting cardholder data and securing payment card transactions

**Scope:** Applies to organizations that process, store, or transmit credit card data

**Key Features:** Network security, access controls, regular monitoring, compliance validation

**Compliance:** Organizations must demonstrate compliance annually to handle credit card transactions

**3. NIST (National Institute of Standards and Technology):**

This standard is developed by the National Institute of Standards and Technology (NIST) in the United States.This provides a risk-based approach to cybersecurity and focuses on five core functions: Identify, Protect, Detect, Respond, and Recover. This standard offers a flexible framework that can be customized to meet the specific needs of organizations and widely adopted in the United States and by organizations working with U.S. government agencies. The highly features are:

**Focus:** Cybersecurity and information security best practices

**Scope:** Provides guidelines, standards, and best practices for various sectors

**Key Features:** Risk assessment, security controls, incident response, security frameworks

**Frameworks**: NIST Cybersecurity Framework (CSF), NIST Special Publications (e.g., SP 800-53)

9. <https://www.iec.ch/international-organizations>

10. <https://www.iso.org/standard/27001>

11. <https://www.techtarget.com/searchsecurity/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard#:~:text=The%20Payment%20Card%20Industry%20Data,misuse%20of%20their%20personal%20information>.

**4. Reserve Bank of India Framework (ReBIT):**

The Reserve Bank, had, provided guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds. [12] The highly features are:

**Focus:** Cybersecurity framework for the banking sector in India

**Scope:** Applicable to banks and financial institutions regulated by the Reserve Bank of India (RBI)

**Key Features:** Cybersecurity controls, risk management, incident response, technology audits

**Compliance:** Banks in India need to align with ReBIT guidelines to ensure cybersecurity readiness

**5. COBIT (Control Objectives for Information and Related Technologies):**

The goal of the COBIT framework is to provide a common language for IT professionals, business executives and compliance auditors to communicate with each other about IT controls, goals, objectives and outcomes. [13] The highly features are:

**Focus:** IT governance and management framework

**Scope:** Provides guidance for aligning IT with business objectives

**Key Features:** Control objectives, management practices, governance processes

**Compliance:** Organizations can use COBIT as a reference to improve their IT governance and control practices

**6. SCF (Secure Controls Framework):**

The SCF is a comprehensive catalog of controls that is designed to enable companies to design, build and maintain secure processes, systems and applications. The SCF addresses both cybersecurity and privacy, so that these principles are designed to be “baked in” at the strategic, operational and tactical levels.[14] The highly features are:

**Focus:** Comprehensive cybersecurity controls framework

**Scope:** Covers a wide range of cybersecurity domains and control families

**Key Features:** Detailed controls, control objectives, implementation guidance

Compliance: Organizations can adopt SCF to establish and maintain robust cybersecurity controls

12. <https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=1721>

13. <https://www.itgovernance.co.uk/cobit>

14. <https://securecontrolsframework.com/start-here/#:~:text=The%20SCF%20is%20a%20comprehensive,strategic%2C%20operational%20and%20tactical%20levels>.

**Comparative Analysis of Cyber Security Standard/Framework**

**Table No 1**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | ISO 27001 | PCIDSS: | NIST: | SecureControlFramework | RBICybersecurity  Framework |
| 1. Scope andApplicability | It provides acomprehensiveframework forinformation securitymanagement systemsapplicabletoalltypes  oforganizations. | Specifically designedfor organizations thathandle cardholder dataor process credit cardtransactions. | Offers a wide rangeof cybersecurityguidelines andframeworksapplicable to variousindustries. | Designed for organizations inthe United States DepartmentofDefense supplychain. | Specifically developed forthebankingsectorinIndia. |
| 2. ComplianceRequirements | Providesrequirements forestablishing,implementing,maintaining, andcontinuallyimproving aninformationsecurity  managementsystem. | Specifies the securitycontrols necessary toprotect cardholder dataduring storage,processing, andtransmission. | Offers a variety offrameworks andguidelines coveringrisk management,incident response,accesscontrols,etc. | Specifies the cybersecuritystandards and controls requiredfor DoD supply chaincontractors. | Provides guidelines forensuring a robustcybersecurity posture inthebankingindustry. |
| 3. Industry Adoptionand Recognition | Widely recognizedand adopted globallyacross variousindustries. | Specifically targeted atthepaymentcardindustry and mandatedbymajorpaymentcard  brands. | Widely adopted andrecognized,especially in theUnitedStatesandby  governmentagencies. | Mandatory for defensecontractorsworkingwiththe  U.S.Department ofDefense. | Mandatory for banks inIndia. |
| 4. Controls andRequirements | Focuses on riskassessment, securitypolicy, assetmanagement, accesscontrol,cryptography,  incident management,etc. | Specifies controls fornetwork security,vulnerabilitymanagement, accesscontrols,encryption,and regular systemmonitoring. | Offers variousframeworks andpublications coveringrisk management,security controls,incidentresponse,etc. | Focused on protectingcontrolled unclassifiedinformation (CUI) in the DoDsupplychain. | Covers areas such astechnology governance,information security,cybersecurity operations,etc. |
| 5. Maturity andContinuousImprovement | Promotes a continualimprovementapproach throughregular audits,reviews, and updatesof the informationsecuritymanagement  system. | Requires annualcomplianceassessments andregular vulnerabilityscans toensureongoingsecurity. | Provides guidelinesfor continuousmonitoring, riskassessment, andincident response toenhancecybersecurity  maturity. | Requires contractors toimplement and maintain acontinuous monitoringprogram. | Encourages banks tocontinuously enhance theircybersecurity posturethrough regularassessments, testing, andtraining. |
| **Limitations** | Its more generic and not specific  Data Privacy, Network device protection, system protection controls are low while internal network protection, system monitoring and asset inventory control, auditing and reporting controls are moderate. | Provides minimal level of controls for  1.Data Privacy  2.Asset inventory controls  3.Auditing & Reporting | 1. Difficult for small organizations to implement. 2. Time consuming for implementation 3. Does not addressed security issues for supply , supply risk management and could computing 4. Policy oriented approach rather than process oriented approach 5. Being technical and complex it poses challenges for small bank with limited IT resources and expertise to implement | It is Robust Cyber security framework. | Limited to financial institutions.  Limited scope for  1. Privacy Protection  Data Sharing, Ownership Policy  2.Use of AI-ML,  3.Cloud Security  4.Situational Awareness  By employing MITRE framework  5.Payment Delivery Channels  SNB, QR, UPI  6.End point Security  7. Vendor Management & SCM  8. More Education to Stakeholders  9. Assessment and Accreditations |

From the table no1, it is revealed that each of these standards and frameworks have its own specific focus, scope, and compliance requirements. Organizations often choose to adopt one or more of these frameworks based on their industry, geographical location, and specific security or regulatory needs. It's important and essential for organizations to evaluate their requirements and select the most appropriate framework(s) to ensure compliance, security, and privacy.

# FINDINGS

When comparing these frameworks, several factors needs to be considered, including the organization's industry, regulatory requirements, and risk profile. However, some general observations can be made:

* NIST CSF and ISO 27001 are more comprehensive and provide a broader scope for overall information security management.
* CIS Controls are highly focused on practical implementation and are suitable for organizations seeking specific guidance on security controls.
* PCI DSS is specifically tailored for organizations involved in payment card processing and focuses on protecting cardholder data.
* Many of the frameworks are not that comprehensive and robust to protect from hackers/fraudsters.
* In India the RBI framework needs to be improvised /refined to overcome the Cyber threats by adding the parameters mentioned in suggestions below.

The suggested additional controls and parameters in the RBI framework are as follows:

* + Robust Privacy and Data Protection measures- Data Sharing, Ownership Policy
  + Use of Artificial Intelligence and Machine Learning
  + Cloud Security framework
  + Situational Awareness By employing and use of MITRE framework
  + Security framework for Payment Delivery Channels- SNB (Social Network Banking),QR (Quick Response Code), UPI (Unified Payment Interface)
  + Endpoint Security
  + Strengthening supply chain risk management
  + Continuous Employee and stakeholder Training
  + Assessment and Accreditations
  + Policy for Cyber Insurance.
  + Policy for Device life Cycle

These suggested inclusions will ensure to mitigate the existing cyber security threats in banking sector.

# CONCLUSION

The study shows that there are many cyber security standards and Cyber Security Frameworks, both are essential for controlling and mitigating Cyber threats. Ultimately, the choice of a cyber security framework depends on an organization's unique requirements, risk appetite, and compliance obligations. Many organizations adopt a mixed/combination of frameworks to achieve comprehensive cyber security practices. More or less this applies to Cyber Security Standards. All the Cyber Security Standards and frameworks need periodic updates, due to innovations in the technology. On these lines the existing RBI framework needs refinement to keep pace with the ever expanding threat surface and evolving threat landscape.

# REFERENCES

# *A.* Journals, Articles and News*.*

1. Cyber Security Standards, Karen Scarfone, Dan Benigni and Tim Grance,National Institute of Standards and Technology (NIST), Gaithersburg, Maryland
2. Deutscher, Stefan & Yin, William & Antonucci, Domenic. (2017). Standards and Frameworks for Cybersecurity. 10.1002/9781119309741.ch6.
3. Tofan, Dan. (2011). Information Security Standards. Journal of Mobile, Embedded and Distributed Systems.
4. Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS-Diah Sulistyowati#, FitriHandayani\*, Yohan Suryanto#
5. A STUDY TO ANALYSE THE IMPACT OF NEW RBI CYBER SECURITY GUIDELINES AND ITS COMPARISON WITH NIST FRAMEWORK, Dr. Nidhi Gupta, International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASSS) 111 ISSN : 2581-9925, Impact Factor: 6.340, Volume 03, No. 03(I), July - September, 2021, pp.111-120
6. EVOLUTION OF CYBERSECURITY STANDARDS IN FINANCIAL SECTORSMadhya Bharti -Humanities and Social Sciences UGC Care Group I Journal, (मध्यभारती) ISSN: 0974-0066 Vol-84 No. 29, January – June: 2023,Published by : Dr. Harisingh Gour University, authored by Dr. Sanjay Shinde, IPS, Dr.Yashwant Patil, Prashant Wadkar
7. An Evaluation Of Security Standards For Online Banking Adopted By Indian Banks Offering Credit /Debit Card Facility Thesis Submitted To The University Of Mysore In Fulfillment Of The Requirement For The Degree Of Doctor Of Philosophy In Commerce By A. M. Sudhakara Research Scholar
8. The Baldrige Cybersecurity Excellence Builder Questions And Self-Analysis Worksheet, See [Www.Nist.Gov/Baldrige/Products-Services/Baldrige-Cybersecurity-Initiative](http://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative).

# Web References:

1. <https://www.educba.com/cyber-security-standards/>
2. <https://cybermagazine.com/cyber-security/history-cybersecurity>
3. [https://en.wikipedia.org/wiki/IT\_security\_standards#:~:text=BS%207799%20part%201%20provides,high%2Dlevel%20guide%20to%20cybersecurity](https://en.wikipedia.org/wiki/IT_security_standards#%3A~%3Atext%3DBS%207799%20part%201%20provides%2Chigh%2Dlevel%20guide%20to%20cybersecurity).
4. <https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework>
5. <https://en.wikipedia.org/wiki/IT_security_standards>
6. <https://www.nist.gov/cyberframework/online-learning/five-functions>
7. <https://gdpr-info.eu/>
8. https:/[/www.rbi.org.in/](http://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=6366&Mode=0)S[cripts/NotificationUser.aspx?Id=6366&Mode=0](http://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=6366&Mode=0)
9. https:/[/www.iso.org/standard/27001](http://www.iso.org/standard/27001)
10. https:/[/www.thehindu.com/news/national/](http://www.thehindu.com/news/national/cert-in-may-be-exempted-from-rti-)c[ert-in-may-be-exempted-from-rti-](http://www.thehindu.com/news/national/cert-in-may-be-exempted-from-rti-) actgovt/article66683021.ece#:~:text=CERT%2Din%20coordinates%20with%20public,vulnerabil ities%20as%20guidance%20for%20organisations.
11. https://listings.pcisecuritystandards.org/documents/pci\_ssc\_quick\_guide.pdf
12. [https://www.statista.com/statistics/1012729/india-number-of-bank-fraud-cases](https://www.statista.com/statistics/1012729/india-number-of-bank-fraud-cases/)
13. <https://economictimes.indiatimes.com/industry/banking/finance/banking/rbi-brings-in-central-fraud-registry-a-likely-major-gamechanger-for-banking/articleshow/70567463.cms>
14. https:/[/www.c](http://www.calyptix.com/hipaa/top-5-cyber-security-frameworks-in-healthcare/)a[lyptix.com/hipaa/top-5-cyber-security-frameworks-in-healthcare/](http://www.calyptix.com/hipaa/top-5-cyber-security-frameworks-in-healthcare/)
15. https:/[/www.bsigroup.com/](http://www.bsigroup.com/en-GB/Cyber-Security/Standards-for-IT-and-cyber-security/)e[n-GB/Cyber-Security/Standards-for-IT-and-cyber-security/](http://www.bsigroup.com/en-GB/Cyber-Security/Standards-for-IT-and-cyber-security/)
16. https://pub.rebit.org.in/2018-09/CMM\_Implementation\_Guide.pdf
17. https://www.ffiec.gov/
18. https://attack.mitre.org/
19. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161219e1.pdf
20. CloudSEK (2020) for RBI Guidelines and NIST Framework 1.1 (2018)
21. Source : https://www.sans.org/webcasts/cybersecurity-standards-scorecard-2022-edition/
22. https://www.youtube.com/watch?v=ADLfKTanxCM
23. https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=1721

# https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=6366&Mode=0

1. <https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf>
2. <https://www.upguard.com/blog/cybersecurity-important>