Cybersecurity Maturity Model

Implementation Guide

Program: Cybersecurity Community Leadership
Initiative: Standards Development - Cybersecurity Maturity Model

Document Type: Public
Document Status: Initial Release
Version: 1.0
Date Last Updated: 28-10-2017

Document Version

Version	Date	Comments
0.1	19/09/2017	Initial Draft
0.2	13/10/2017	Minor editorial changes
1.0	28/10/2017	First release

Contributing Members

Memeber	Current Role
Mr. Ashutosh Jain	CISO, AXIS Bank
Mr. Deval Majumdar	CISO, Indusind bank
Mr. Jaspal Singh Sawhney	CISO, Deutsche Bank
Mr. Murli Nambiar	SrVP, Cybersecurity, ReBIT
Mr. Sameer Ratolikar	CISO, HDFC Bank
Mr. Subhash Subramaniam	CISO, ICICI Bank
Mr. Vishal Salvi	CISO, Infosys
Mr. Vivek Srivastav	SrVP, Research & Innovation, ReBIT
Mr. YV Ramana Murthy	CISO, SBI
Mr. Rajesh Hemrajani	CISO, IDFC Bank
Mr. Nabojyoti Sarkar	ICICI
Mr. Manoj Kuruvanthody	Infosys
Ms. Aparna B	SBI
Mr. Mukund Inamdar	HDFC Bank
Prof. Sunil Bakshi	NIBM
Mr. Jayaraman Pazhamalai	SrVP, System Audit, ReBIT

Acknowledgements:
Suhas Desai (Aujas), Anand Naik (Sequretek), Anupama Narayanan (ReBIT), Vinay Jain (ReBIT), Karthik Bappanad (ReBIT)

Table of Content

1 Introduction

There have been several regulatory and industry initiatives to define the cybersecurity framework for banks. The Reserve Bank of India (RBI) set up an expert committee, under Mr G Gopalakrishna, which released its recommendatory report in January 2011 [1]. RBI further issued a circular on cyber security framework (RBI-CSF) in June 2016 [2]. In addition, Institute for Development and Research in Banking Technology (IDRBT) has worked through industry initiatives and has defined "Information Security Framework [3]" and "Cyber Security Checklist [4]". Several international initiatives are also of note in this area, such as work by National Institute of Standards and Technology (NIST) and Federal Financial Institutions Examination Council (FFIEC) [6] in USA and Hong Kong Monetary Authority (HKMA) Cyber Resilience Assessment Framework (C-RAF) model in Hong Kong.

While the international frameworks and guidelines provide useful descriptions of capabilities, controls, processes and awareness, they may not be directly applicable to Indian banks, as they do not describe the approach and the path firms need to take to evolve their maturity in these areas. Furthermore, they have been developed as self-help tools and do not focus on benchmarking and providing a regulatory tracking of assessment. It is also observed that there is a lack of uniformity and firms interpret the cybersecurity frameworks differently. Also, auditors struggle to justify the scope of audit and often there are efforts to comply but not in spirit. Furthermore, the firms do not know if their security-related investments are adequate or if they do not suffice. To address these and promote uniformity in standards adoption, this Cyber Security Maturity Model (CMM) has been developed, as an industry initiative and coordinated by ReBIT. The CMM will provide guidance through:

- Methodical approach to measurement of risk, planning of controls and governance and security strategy execution to strengthen cybersecurity posture of financial firms
- Metrics based treatment, benchmarking and prioritizing risk driven investment in security

Thus, the purpose of the cybersecurity maturity model is to further the implementation and adoption of the mandated cybersecurity framework uniformly in the financial firms and understanding of the firm's cybersecurity maturity in terms of the adoption of the regulatory cybersecurity framework.

In addition, the Cyber Security Maturity Model will help the financial firms address their security gaps, plan a security roadmap through clear guidance, assessment and best practices, enable benchmarking and help firms make strategic investment decisions in cyber security core domains in conformity to their business needs and risk appetite. The model will also help develop additional specifications, best practices and tools in a structured manner.

While this document assumes the scope based on the RBI-CSF, it is acknowledged that the cyber resiliency requirements may change with time [2]. In this context the model aspires to

withstand the test of time and adapt to any new changes. The working group also acknowledges that the framework has to be harmonious with international standards, such as NIST CSF, COBIT 5.0 [8], ISO 27000 [9] and other standards.

This document is the implementation guide for the Cyber Security Maturity Model. It will help firms understand the CMM spreadsheet tool and complete the self-assessment process. The CMM spreadsheet tool will be built into an online tool eventually after feedback and initial industry adoption. As such the process will evolve. The most up to date information will always be made available on ReBIT's website at https://rebit.org.in. Any comments/concerns may be submitted to communications@rebit.org.in.

1.1 Document Structure and Conventions

The Cyber Security Maturity Model artifacts comprise of this document and a separate CMM spreadsheet tool [TODO: ref]. This implementation guide provides overview, organization and structure of the CMM tool and thus is a supplemental document to understand the CMM tool. While the CMM tool is operational, this document provides the underpinnings of the approach taken to arrive at the model and defines the CMM architecture.

The spreadsheet uses certain color coding conventions:

	These are cells that are not editable and may report the values or provide descriptions
	These cells are internal cells used for computing the values
	These cells are user input cells

Wherever the CMM tables are referenced, this color coding scheme is followed.

In addition, the document also uses the NIST color coding conventions [7], as shown below:

Identify
Protect
Detect
Respond
Recover

It is recognized that several firms may operate in different regulatory regimes and consequently may need to comply with various international security standards and framework. NIST model is adopted by many international and domestic organizations. These

color coding will help firms align their security postures with NIST accordingly. Similarly a mapping of COBIT 5 with RBI's Cybersecurity Framework, albeit not directly used in the model is referenced [11]. These various mappings would assist a firm to meet varied needs of various regulatory regimes and ease their assessment and compliance burden. That said, it needs to be emphasised that this CMM document derives its strength from the contributions from the members operating primarily within RBI-CSF.

The Chapter 2 describes the international work and efforts in this area. Chapter 3 discusses the RBI-CSF and provides a high level overview which forms the underpinning of the CMM. Chapter 4 outlines the Cybersecurity Maturity Model structure, describes risk, maturity and effectiveness assessment structure and general overview. Chapter 5 describes the categorization of inherent risk, assessment model, maturity levels and scoring model and thus lays the foundational structure on which the CMM is built. Chapter 6 describes the organization of the assessment areas into logical domains. Chapter 7 outlines the mechanisms of the operational effectiveness measurement and Chapter 8 describes the scoring and reporting mechanisms.

The key terminologies in the document uses the `consolas` font. Rest of the document uses Lucida Sans.

1.2 Terms and Definitions

This document defines and uses some new terminology to define the model. The terms as used in the document are defined below:

`Core Domains`	The `Core Domains` represents a logical grouping of cyber security related functions that firms would undertake. The model defines five cyber security domains defined in Chapter 6.
`Control Areas`	The `Control Areas` are specialized areas of operation or process in which the maturity is to be measured, so a focussed improvement can be planned.
`Control Principles`	Each of the `Control Area`, may have multiple mechanisms and controls that can be assessed separately or form a logical group, these are called "`Control Principles`" in the maturity model. The `Control Principles` are specific controls that may be related to people, process or technology aspect of improving maturity for the parent `Control Area`.
`Cybersecurity`	The term `Cybersecurity` implies controls and principles through use of process, procedures, awareness, governance and technology to secure the operations and

	physical and digital assets and environment of an organization.
Inherent Risk	The Inherent Risk is risk arising of the area of business operations, size and number of external touch points. It is independent of process, controls and technology the organization may put in place. Understanding the Inherent Risk is important for determining the maturity levels of the target.
Maturity Assessment	The Maturity Assessment is the process of identifying the level of maturity based on the Control Principles defined. Each Control Principle is defined with five progressive levels of maturity.
Operational Effectiveness	While the Control Principles are a self-assessed mechanism to understand and plan improvements in a particular Control Area, the Operational Effectiveness measures the on-the-ground realities to assess the adoption and execution of the Control Principles. Thus the Maturity Assessment may be subjective to some extent, but Operational Effectiveness is objective.
Inherent Risk Score	A consolidated single number on a scale of 1-100 will provide the Inherent Risk Score. Higher number indicates the need for better risk and maturity.
Maturity Assessment Score	A consolidated number on a scale of 0-500 will provide a final Maturity Assessment Score after the self-assessment representing maturity across the applicable and assessed Control Areas.
Operational Effectiveness Score	A consolidated number on a scale of 0-500 will provide a final Operational Effectiveness Score after the self-assessment representing maturity across the applicable and assessed Control Areas. The final Operational Effectiveness Score is computed based on individual “Implementation Compliance Score” for areas covered in the Operational Effectiveness worksheet.

2 International work in this area

2.1 FFIEC Model

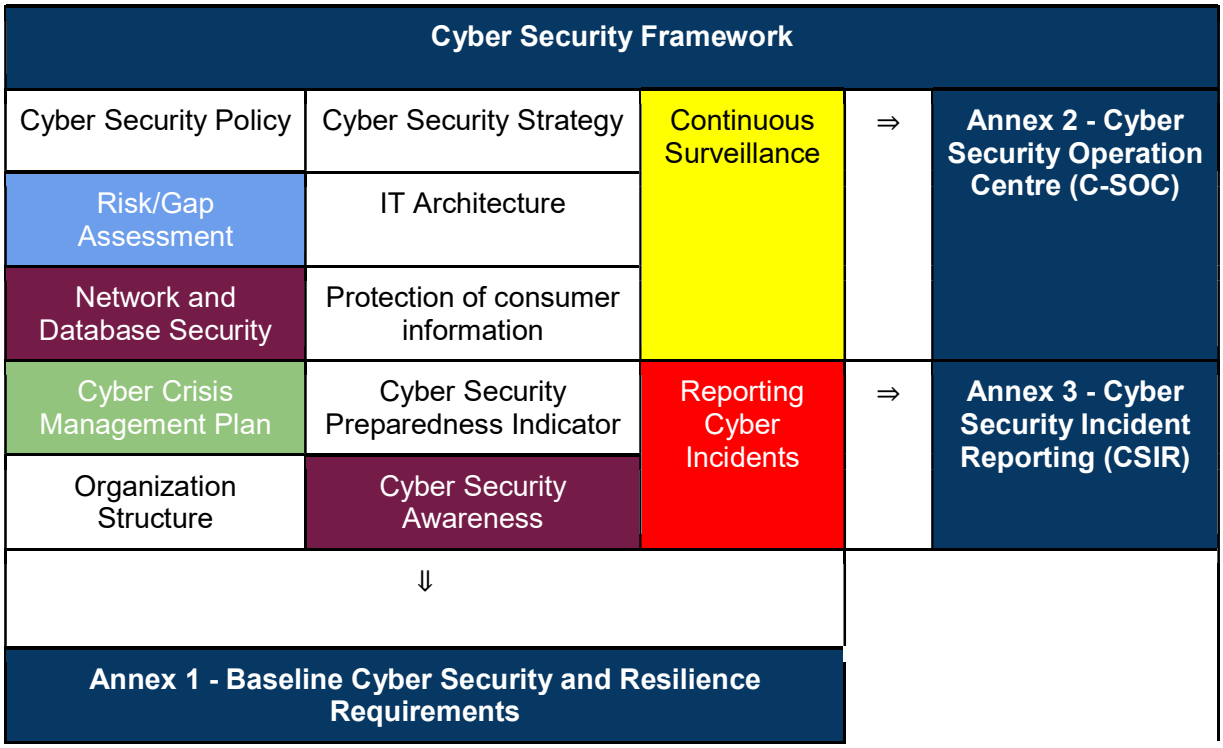
The FFIEC Cybersecurity Assessment Tools [6] maps the core domain against inherent risk.

2.2 HKMA Model

The Hong Kong Monetary Authority has published a Cyber Resilience Assessment Framework (C-RAF) that enables financial firms to assess the maturity in 25 components across 7 domains namely, Governance, Identification, Protection, Detection, Response and Recovery, Situational Awareness, and Third Party Risk Management.

3 RBI's Cyber Security Framework

The RBI Cybersecurity Framework (RBI-CSF) coverage is shown below. The CMM provides a mapping to the framework.



Color coding as per the NIST framework. NIST framework does not define a separate governance area. These areas in the above diagrams are identified in white color background.

4 CMM Development Model

The Cyber Security Maturity Model encompasses four key segments. These four segments describing the scope, risk, assessment and effectiveness comprises the overall scope of the Cyber Security Maturity Model.

Core Domains	Inherent Risk
The core domains areas broadly classify the various control areas into logical groups. The Model defines five Core Domain areas. Each of the domain has multiple Control Areas, based on thematic categorisation for assessing maturity in a particular area to track and assess process and operational effectiveness. The "Control Areas" are further sub-divided into "Control Principles" for maturity assessments.	The "Inherent Risk" of an organization depends upon the products and services that it operates, the assets that are needed to provide financial services to its customers, the delivery channels it uses, and its track record on cyber incidents.
Maturity Assessment	**Operational Effectiveness**
The Maturity Assessment enables a financial institution to assess its process and controls maturity. The "Maturity Assessment" defines "Controls Principles" with five progressive levels of maturity.	The "Operational Effectiveness" measures the effectiveness of the firm in implementation of the "controls" in the various "Control Areas". The "Operational Effectiveness" is assessed only in areas where metrics are available.

Thus the Cyber Security Maturity Model broadly assesses three main things across the "Core Domain" areas as shown in the figure below.

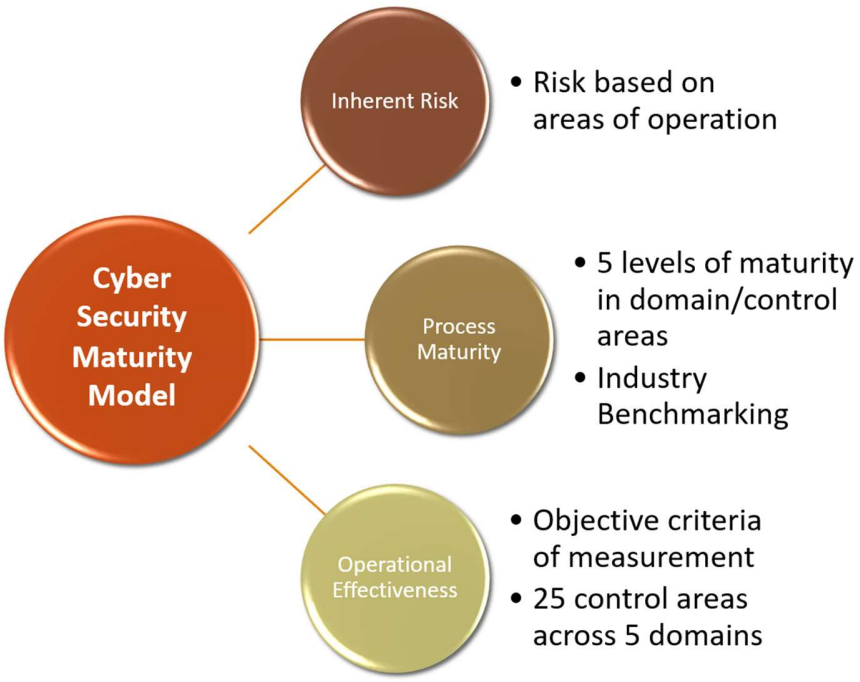


Fig. 2.1 CMM three main assessment types

The following diagram shows relationship between various CMM segments. These relationships help establish the mechanisms for 3 types of aforementioned assessments. While the "`Inherent Risk`" measures the risk based on business operation, the "`Maturity Assessment`" and "`Operational Effectiveness`" are related to the assessments logically grouped by "Control Areas".

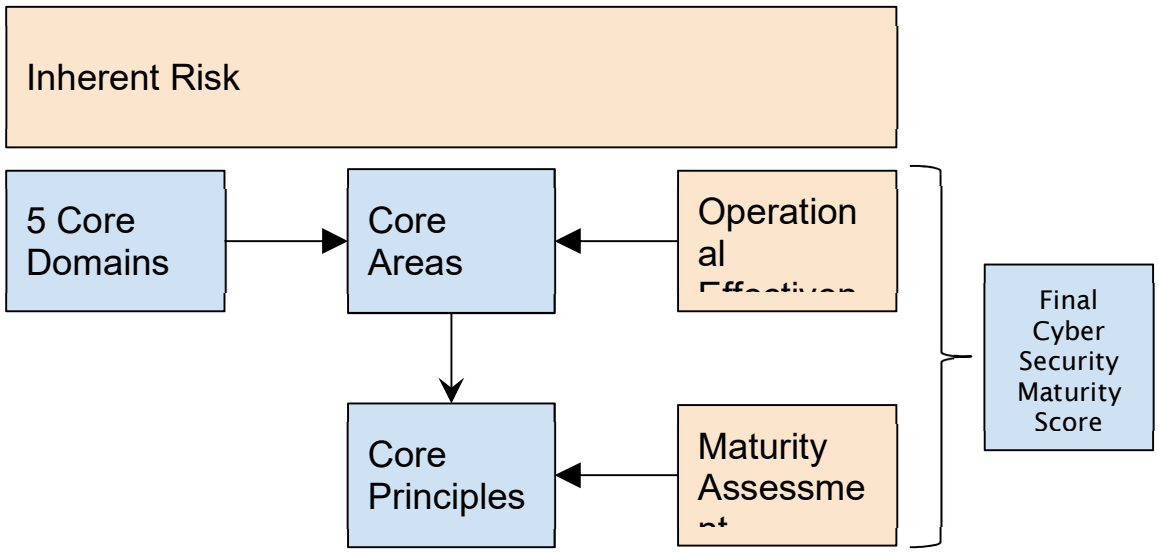


Fig. 2.2 Relationships between the CMM segments

The CMM also provides mapping to various standards and specifications. Each of the "Control Principle" is mapped to various standards. In the initial draft mapping to the following standards are considered.

Standards						
RBI		NIST	ISO 27001			
Gopalakrishna Committee	Cyber security Framework	NIST Sub-Category	ISO 27001:2013 Control No.	ISO 27001 Domain	IDRBT	DSCI

Since the CMM will also be used for benchmarking and comparative analysis, it is desirable to group similar organizations together. In this context a concept of "Business Profile" is used. The model itself, as defined in the CMM assessment spreadsheet, does not encapsulate any requirements for organization to assess their business profile, but lists areas of business operations pertinent to the organization. Furthermore the "Business Profile" may be used to assess the "Inherent Risk". The concept of "Business Profile" is implicit in the model.

4.1 Core Domains

The following table below describes the five Core Domain areas, the respective Control Areas and their definitions.

Table 4.1

#	Core Domains
1	Security Management
2	Infrastructure Management

3	Cybersecurity Engineering
4	Delivery Channels
5	Situational Awareness

The Core Domains enable a firm to logically group people, process and technology aspects of cybersecurity control areas to appropriately assess and measure maturity score levels in these areas and thus provide guidance on those areas and the others which need improvement.

The Core Domain areas are further divided into 25 Control Areas. The following diagram shows the split of the domain areas.

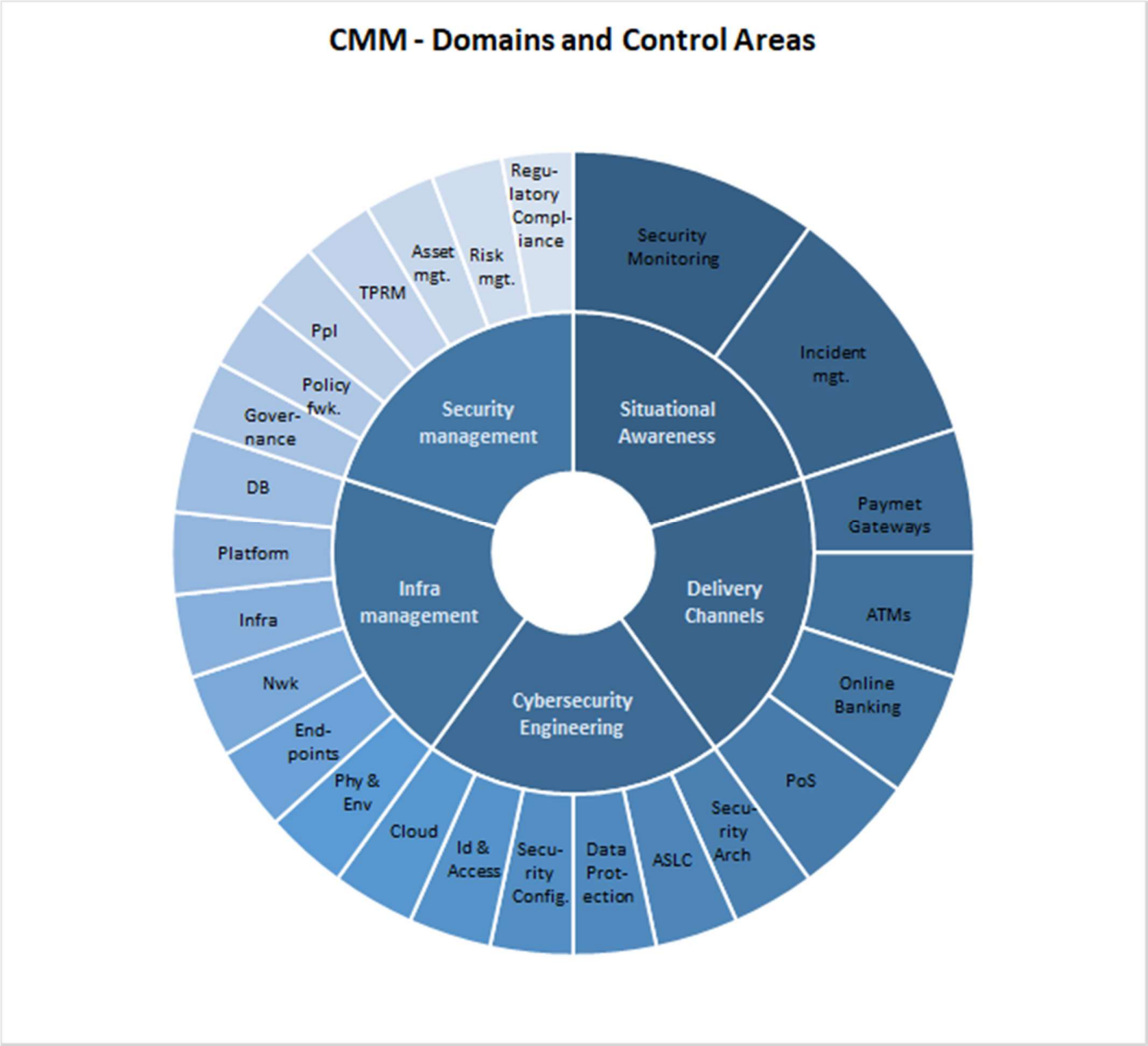


Fig. 4.1 CMM Domains and Control Areas

5 Cyber Security Preparedness, Maturity Levels and Profiles

5.1 Inherent Risk Categories and Levels

The operation of a firm exposes it to cyber risks. The cyber risk itself is difficult to measure because of various negative externalities and difficulty of accessing indirect costs associated

with cyber incidents. The inherent risk is a measure that will enable the organization to quantify a risk because of its business operation.

The first step in the self-assessment using the CMM tool is to evaluate the Inherent Risk of the firm. The inherent risk relates to business risk a firm is exposed to based on its size, area of operation, but irrespective of controls, policies and its own security postures. The inherent risk assessment is important because, it gives an indication about what level of maturity is adequate for the organization. Higher the Inherent Risk, higher the requirement for maturity level. Organizations with similar inherent risk profiles may be grouped together to provide a better benchmarking of the maturity levels needed in their peer group.

The inherent risk is grouped into the following four assessment categories:

Table 5.1

Inherent Risk Assessment Areas
Category-1: Technology
Category-2: Delivery Channels
Category-3: Products and technology services
Category-4: Tracked record on cyber threats

5.1.1 Inherent Risk Levels

The Inherent Risk is based on objective measures on indicators defined in each of these four categories. The CMM tool provides guidance on how to select the risk levels. The following levels are applicable:

Table 5.2

Inherent Risk Levels
Low
Medium
High
Not Applicable

5.2 Maturity Assessment

The second step in the CMM self-assessment is evaluation of firm's level of maturity in the core domain areas. Each `Core Domain` contains one or more "`Control Areas`" which are further logically subdivided into "`Control Principle`" areas. These are defined in the following sections.

5.2.1 Maturity Assessment Levels

The Maturity Assessment is broadly classified in the following levels and scoring:

Table 5.3

Maturity Assessment Rating		Description
Missing Control Strategy	0	Control strategy is not defined.
INITIALIZING	1	Processes unpredictable, poorly controlled and reactive
DEVELOPING	2	Processes characterized for projects and is often reactive
OPERATING	3	Processes characterized for the organization and is proactive
MANAGING	4	Processes measured and controlled
OPTIMIZING	5	Focus and process improvement

These maturity assessments are defined in the following diagram:

Fig. 2.3 The Process Maturity Levels

Each of the "Control Principles" is classified into one of these aforementioned levels. The general principles used to define the maturity levels is provided in Table 5.3. They represent incremental level of a firm's capability in strengthening their cybersecurity posture. For example, when a firm assesses itself at L4, the maturity defined in the preceding levels i.e. L1, L2 & L3 is assumed. In rare cases, it may appear that a firm's capabilities meet the control requirements defined at a certain maturity level, but do not completely meet control requirements defined in a preceding maturity level. In such cases, careful review and documentation should highlight such exceptions before assessing the firm at a higher level of maturity.

The financial firms would be able to determine maturity levels on the basis of inherent risks needed for specific assessment area. For example, if the a firm has significant risk in a specific preparedness assessment area, but the maturity level is found to be "**Evolving**", then the firm is "**under invested**" and needs to invest more to strengthen the maturity level to at least **Advanced**. If on the other hand, the firm's preparedness risk is found to be "Least", but the firm has got "Advanced" practices and controls in place, the firm has "**invested in excess**".

5.3 Scoring Model

The scoring will be in the range of 1-5 for each "`Control Area`". The weightages may be further divided into one or more of the "`Control Principles`" within the "`Control Area`".

The following table below shows the sample mechanisms of the assessment process. The self-assessment would require identification by the assessor whether the control is applicable or not and selection of `Maturity Assessment` as defined in section 5.2.1. A score will be computed for that given control principle based on weightage assigned to the control principle. This computed assessment score will then be consolidated in the final Maturity Assessment Result.

Control Areas --> Control Principle		Applicable [Y]/[N]	Maturity Assessment	Computed Assessment Score
1.1	**Cyber Governance**			

1.1.1	**Cyber Security Framework** The cyber security framework deployed in bank takes following aspects into consideration: - Alignment with business objectives and the legal requirements - Information security roles and responsibilities - Periodic reviews of the policy and review of compliance against policy - Tracking of non-compliances and reporting L1: The bank has identified a cyber security framework to create, track and manage processes relating to cyber security. This framework is updated as per need basis. L2: The bank has identified and updated the framework on the basis of personnel inputs and updates received by the bank. Actionable items are drawn and communicated to concerned teams to manage and address the requirements. L3: The bank has defined a framework for cyber security to address alignment of business and legal requirements, along with roles and responsibilities of personnel documented and mechanism implemented for periodic reviews and tracking non-compliance in the bank. Any new and existing changes in the framework is addressed. All the concerned teams are communicated on their duties. L4: The bank has incorporated regular updates to management in the defined framework. Review meetings are conducted to address the actionables. All the actionables are time bound and tracked. Self-Assessments are performed regularly. L5: The bank has liaison with industry experts for updates and pre-emptive inputs on changing landscape to update the policy.	Y	Policy Defined	1

6 Cyber Security Domains

6.1 Security Management

The Security Management Area comprises of 7 different `Control Areas`. The following table describes each of these control areas.

Core Domains		Control Areas	Definitions
Security Management	1.1	Cyber Governance	Cyber security governance in the bank comprises of the responsibilities and engagement of Board of Directors and senior management, organizational structures, and processes that protect information and mitigation of growing cyber security threats. Cyber security governance ensures alignment of cyber security with business strategy to support organizational objectives.
	1.2	Policy Framework	Cyber-security policy framework elucidates the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk, duly approved by their Board.
	1.3	People and Awareness	A cyber security technology or process is only as effective as the knowledge of people and their awareness about it. Organizations should provides periodic trainings on cyber risk management to ensure all personnel have necessary knowledge about the risk management process. This domain considers maturity and effectiveness of the cybersecurity training and awareness programs instituted by an organization.
	1.4	Risk Management	The cyber risk comprises of various business and strategic risk that arises out of cyber security concerns. The overall Risk Management should include assessment,

		Cyber Crisis Management Plan (CCMP), Business Continuity(BC) & Risk Management and Mitigation Plans.
1.5	Asset Management	A centralized asset management and inventory process is required to effectively manage system patches, prevent misuse and data leakage. The asset management domain considers whether the regulated entity is maintaining up-to-date inventory of all assets including applications, Tangible and intangible information assets which are associated with any or all kind of information and information enabled services containing parameters such as but not limited to ownership, classification of the assets.
1.6	3rd Party Risk Management	The domain covers Centralized Vendor Management Office, vendor training, SLA agreement that comprises of rules of engagement in cyber crisis.
1.7	Regulatory Compliance	This domain enumerates all the regulatory compliance requirements related to cybersecurity. Regulatory compliance requires that the bank has recognized the applicable legislation and regulatory compliance they need to adhere to and has implemented necessary controls.

6.2 Infrastructure Management

The infrastructure management comprises of 6 different `Control Areas`. The following table describes each of the control areas.

Infrastructure Management	2.1	Physical and Environment Security	A good access control strategy also involves physical and environment security. The premise management

			maintains details of safety of personal and company's assets critical to ensuring preventive steps against threats which may can arise out of sabotages and other intrusions. This also covers having redundancy and resilience via DR capabilities.
	2.2	Endpoint Security	The Endpoint Security control area comprises all endpoint devices connected to the network such as, but not limited to, laptops, desktops, mobile devices, IoT devices, telephones, printers and similar IT peripherals.
	2.3	Network Security	The Network Security area comprises of all network devices such as, but not limited to, routers, switches etc.
	2.4	Infrastructure Security	Comprises of Servers specific Security aspects
	2.5	Database security	Database security concerns the use of a broad range of information security controls to protect databases (potentially including the data, the database applications or stored functions, the database systems, the database servers and the associated network links) against compromises of their confidentiality, integrity and availability. It involves various types or categories of controls, such as technical, procedural/administrative and physical. Database security is a specialist topic within the broader realms of computer security, information security and risk management. [wikipedia]
	2.6	Platform Security	The security best practices needs to be applied to the hardware and the operating systems on which the applications run. Many device/equipment provides provide default credentials, the systems may

			require some additional setups to make it more secure. The platform security covers areas such as OS and device hardening mechanisms. Management of EOL products etc.

6.3 Cybersecurity Engineering

The Cybersecurity Engineering domain has 6 different `Control Areas`.

Cybersecurity Engineering	3.1	Security Architecture	The security architecture covers areas that organizations should cover to strengthen the security of the enterprise system as a whole. DNS Governance, Anti-phishing controls, enterprise security design, API management and governance are some of the areas.
	3.2	Data Protection	The data protection relates to securing the data at rest, data in motion and access to the data. This is an important control area that include data classifications, DLP mechanisms, data lifecycle management, data retention policies, and data tokenization.
	3.3	Identity and Access Management	This control covers mechanisms that "enables the right individuals to access the right resources at the right times and for the right reasons". Password Management and PIM are integral to identity and access management.
	3.4	Security Configuration	Platform related configurations, PSB(Platform security baselines, device and environment hardening).

	3.5	Application Security Life Cycle	Majority of the incidents happen because of poor application design, inadequate security consideration either in design or in configuration of the system. This domain covers the application security life cycle that includes secure software development, threat modeling, security requirements, and OWASP framework. Application Security Lifecycle Management will cover Application Security. Secure Software Development Lifecycle will cover Security Testing & System Development. Stress is laid on Top-10 OWASP testing.
	3.6	Cloud Security	Leveraging cloud is possible through several models. Organizations may use cloud infrastructure to run their services. They may use other SaaS provides for either integration or for business processes and support services. The control area considers maturity model of an organization in adopting the challenges in such environment. There are public, private and hybrid models and these may require different security considerations as the traditional perimeter based security model may be inadequate or used to collect logs and testing may be different from the traditional application or enterprise security models.

6.4 Delivery Channels

The Delivery Channels domain has 4 "`Control Areas`".

Delivery Channels	4.1	Payment Gateways / Channels	The online e-commerce and retail transactions are processed through the payment gateways. These PSPs directly interact with customer's bank to process the payment. The UPI, mobile wallet and

			other modes of digital payments are covered in this section. The security and maturity of the ecosystem is covered in this control area.
	4.2	ATMs	ATM security is and maturity is covered in this section.
	4.3	PoS systems	Point of Sale system security is covered in this section.
	4.4	Online & Mobile Banking	The web and mobile applications that provide consumers to access their account and perform certain banking functions and services are covered in this section.

6.5 Situational Awareness

The Situational Awareness domain has 2 "`Control Areas`".

Situational Awareness	5.1	Security Monitoring	The domain covers SOC operation and any advanced analytics that may use network anomaly or user anomaly detection.
	5.2	Incident Management	The incident management domain includes threat intelligence services, incident analysis, incident lifecycle management, incident response and regulatory reporting.

7 Measuring Operational Effectiveness

The `Operational Effectiveness` measurement computes how effectively the maturity principles are being applied within the organization by evaluating it against the coverage. A 100% coverage of the maturity principles would imply an implementation compliance score of 100% based on objective criteria.

In certain "`Control Areas`" the "`Operational Effectiveness`" can't be measured through any metrics. In such scenarios, the "`Operational Effectiveness`" work-sheet will not have any details on the control and the CMM tool will yield a implementation score of 100%. The "`Operational Effectiveness`" will map to key risk indicators and evolve dynamically over period of time.

An example of the operational effectiveness measurement worksheet is shown below.

#	Controls	Description of the Control	Effectiveness Parameters		Individual Weighted Effectiveness Score
			Weightage	Coverage	
1.3.1	People and Awareness	Training: % of employees with security trainings at different levels	8	70%	70%

8 Scoring and Reporting

The CMM will provide a self-assessed maturity score and an Operational Effectiveness Score. The scores are computed based on the "`Maturity Assessment`" and "`Operational Effectiveness`" sheets. The Maturity Assessment Score is a weighted average score of various different "`Control Principles`" defined for that particular "`Control Area`". The following sample table illustrates this further.

Domain	Controls	Maturity Assessment Score	Implementation Compliance Score
Security Management	Cyber Governance	0	100%
	Policy Framework	0	100%
	People and Awareness	0	70%
	Risk Management	0	70%
	Asset Management	0	75%
	3rd Party Risk Management	0	72%
	Regulatory Compliance	0	70%

The consolidated score for each of the cyber security domain is computed based on the average and a final score is computed based on `Maturity Assessment` and the `Operational Effectiveness Score`.

8.1 Benchmarking

It would be possible to define an industry benchmarking based on statistical data once financial firms start sharing their results.

The following spider chart shows an example of an infographic that can be produced for the firm based on the industry benchmarking.

8.2 Management Reporting

The management report should be comprehensive and reflect the firm's maturity profile and corresponding score with suggested areas of underinvestment. The respective score in each of the domain area and the corresponding benchmarking will enable the firm to make a data driven investment decision in security. Following three consolidated scores will be generated from the self assessment:

- Inherent Risk Score
- Maturity Assessment Score
- Operational Effectiveness Score

These three consolidated scores will be rolled up into a single maturity score in the range of [0-500].

Furthermore, the industry benchmark as described in section 8.1 will form the basis of management reporting.

9 References

[1] Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds, https://rbi.org.in/SCRIPTs/BS_CircularIndexDisplay.aspx?Id=6366 (RBI/2010-11/494 DBS.CO.ITC.BC.No. 6/31.02.008/2010-11) dated Apr 29, 2011

[2] RBI Cybersecurity Framework, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF

[3] Information Security Framework, IDRBT, 2012 http://www.idrbt.ac.in/assets/publications/Best%20Practices/IDRBT_ISFW_2012.pdf

[4] Cyber Security Checklist, IDRBT, July 2016 http://www.idrbt.ac.in/assets/publications/Best%20Practices/CSCL_Final.pdf

[5] Press Release: 2016-2017/2127, Statement on Developmental and Regulatory Policies , Feb 8th, 2017

[6] Federal Financial Institutions Examination Council: Cybersecurity Assessment Tool was issued on On June 30, 2015 and is available at the following URL: https://www.ffiec.gov/cyberassessmenttool.htm

[7] NIST Cyber Security Framework, https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1-with-markup.pdf

[8] COBIT 5.0, https://www.isaca.org/cobit/pages/cobit-5-framework-product-page.aspx

[9] ISO 27000, Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary, http://standards.iso.org/ittf/PubliclyAvailableStandards/

[10] Scott, LouAnn. "Baldrige Cybersecurity Initiative." *NIST*. 09 Mar. 2017. Web. 13 Mar. 2017. https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative

[11] COBIT 5 RBI Framework Mapping, Prasad Pandse, ISACA, Version 1.1, 16th Jan 2014, https://www.isaca.org/Groups/Professional-English/india/GroupDocuments/COBIT%205_%20RBI_Guidelines_Mapping_Tool_version%201.1.xls

[12] ReBIT's Operational Excellence Webinars, http://webinar.rebit.org.in

9.1 Annex 1 - Baseline Cyber Security and Resilience Requirements

Annex 1 - Baseline Cyber Security and Resilience Requirements				
Inventory Management of Business IT Assets	Preventing execution of unauthorized software	Environmental Controls	Network Management and Security	Secure Configuration
Application Security Lifecycle (ASLC)	Patch/Vulnerability & Change Management	User Access Control/ Management	Authentication Framework for Customers	Secure mail and messaging systems
Vendor Risk Management	Removable Media	Advanced Real-time Threat Defense and Management	Anti-Phishing	Data Leak Prevention Strategy
Maintenance, Monitoring, and Analysis of Audit Logs	Audit Log Settings	Vulnerability assessment and Penetration Test and Red Team Exercises	Incident Response & Management	Risk based transaction monitoring
Metrics	Forensics	User/Employee/ Management Awareness	Customer Education and Awareness	