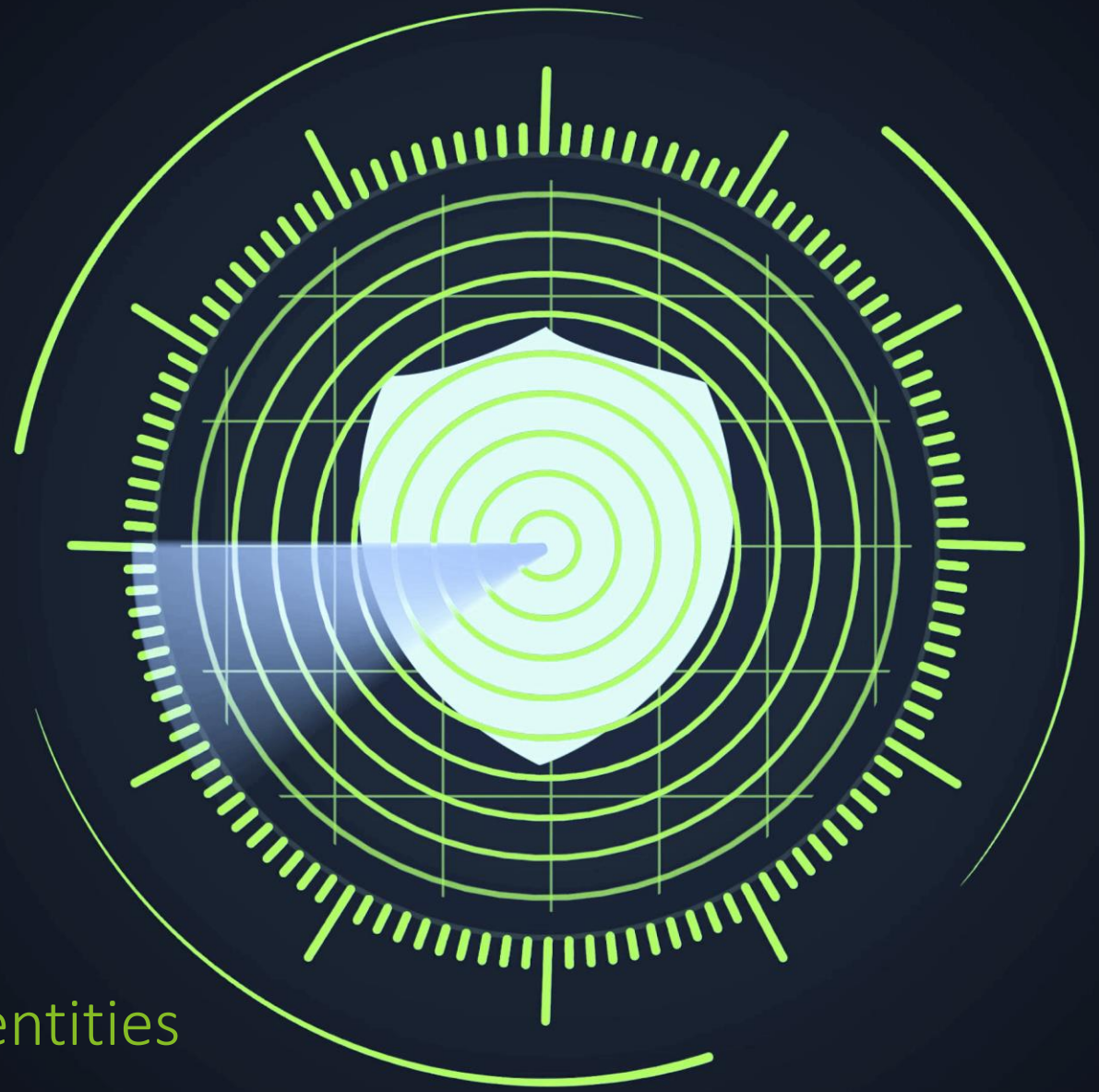
Deloitte.



Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI-regulated entities

Point of View | September 2024

Introduction

Rapid growth in IT usage in the securities market—a critical component of The Securities and Exchange Board of India (SEBI) Regulated Entities (REs).

Technological advancement and the protection of IT infrastructure—key concerns for SEBI REs.

Since 2015, SEBI has issued cybersecurity and cyber resilience frameworks for various REs.

20 August 2024- SEBI issued a "Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI REs" reviewed by SEBI's High Powered Steering Committee (HPSC– CS).

The framework

04 sections

- Part I: Objectives and standards
- Part II: Guidelines
- Part III: Structured formats for compliance
- Part IV: Annexures and references

02 approaches

- Cybersecurity: Governance measures to operational controls
- Cyber resilience goals: Anticipate, withstand, contain, recover and evolve

CSCRF: Need of the hour

SEBI REs have increased their technology adoption in recent years. With the fast pace of technological developments in the securities market, maintaining robust cybersecurity and cyber resilience to protect REs' operations from cyber risks and cyber incidents has become necessary.

Why

SEBI released the CSCRF to address the growing risks and difficulties related to cybersecurity in the financial markets. The following are this framework's main goals:

- Enhance cybersecurity measures
- Ensure cyber resilience
- Standardise cybersecurity practices
- Promote risk management
- Encourage regular assessments
- Strengthen incident reporting

Who

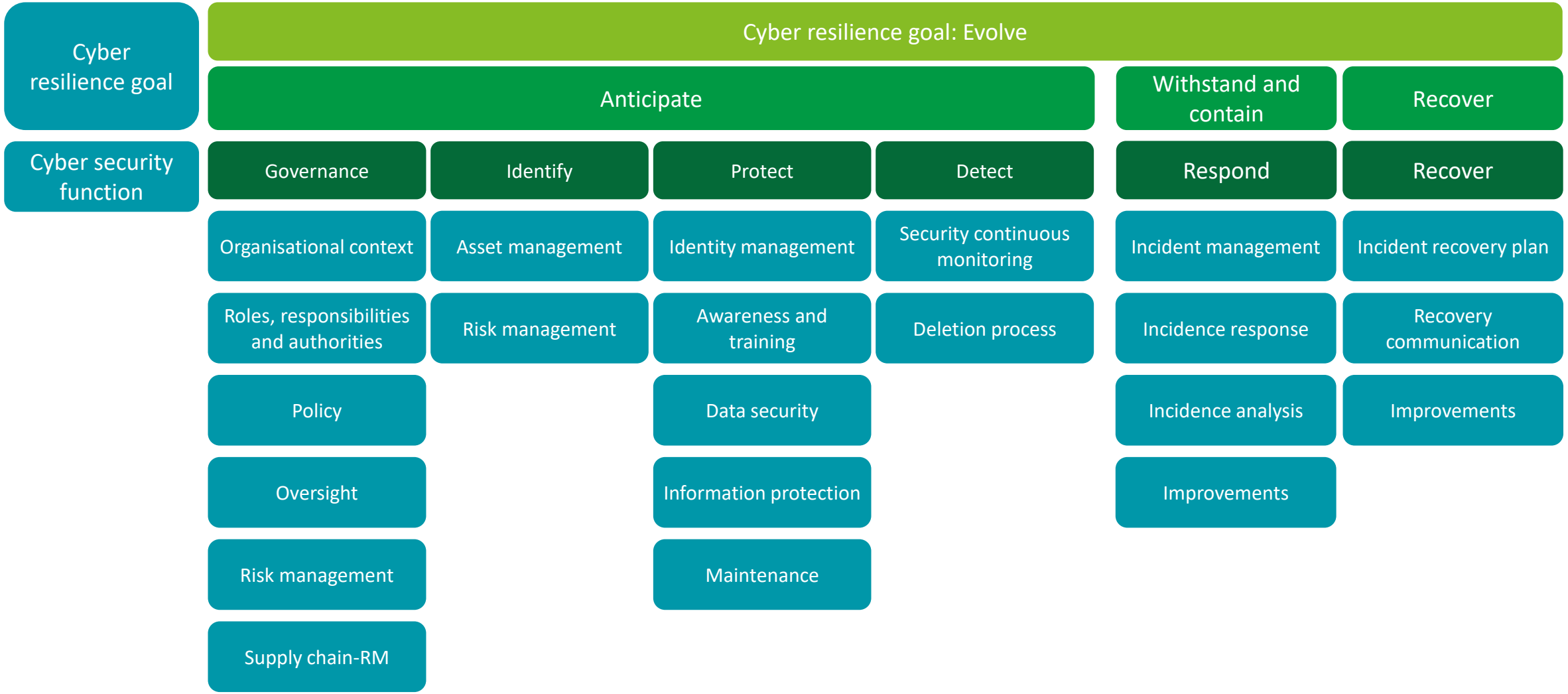
- Alternative Investment Funds (AIFs)
- Merchant Bankers (MBs)
- Clearing corporations
- Collective Investment Schemes (CIS)
- Custodians
- Debenture trustees
- Depositories
- Designated depository participant
- Depository participants through depositories
- Investment advisors
- Mutual funds
- Portfolio managers
- Registrar to an issue and share transfer agents
- Stockbrokers through exchanges
- Stock exchanges
- Venture Capital Funds (VCFs)
- Research analysts
- KYC Registration Agencies (KRAs)
- Bankers to an issue (BTI) and Self-Certified Syndicate Banks (SCSBs)

When

REs are required to comply with the standards and mandatory guidelines mentioned in the CSCRF Below are the timelines for the adoption of CSCRF provisions:

- For six categories of REs where "cybersecurity and cyber resilience circular" already exists—by 1 January 2025
- For other REs where CSCRF is being issued for the first time—by 1 April 2025

CSCRF: Overview



What does this framework supersede?

The CSCRF aims to provide standards and guidelines for strengthening cyber resilience and maintaining robust cybersecurity of SEBI REs. Its key objectives are to address evolving cyber threats, align with industry standards, encourage efficient audits and ensure SEBI REs' compliance.

The consolidated **CSCRF will supersede 08 SEBI circulars and 20 letters/advisories**.

Following are the superseded SEBI circulars

01 **Market Infrastructure Institutions (MIIs):** CSCRF of stock exchanges, clearing corporations and depositories (August 2023)

02 **Stockbrokers/Depository participants:** CSCRF for stockbrokers/depository participants (June 2022)

03 **Mutual funds/Asset Management Companies (AMCs):** CSCRF of mutual funds/asset management companies (June 2022)

04 **Portfolio managers:** CSCRF for portfolio managers (March 2023)

05 **KRAs**: CSCRF of KYC registration agencies (July 2022)

06 **QRATAs:** CSCRF of Qualified Registrars to an Issue and Share Transfer Agents (QRTAs) (July 2022)

07 **All regulated entities** (February 2023)

08 **Stock exchanges, clearing corporations and depositories** (except commodities derivatives exchanges and their clearing corporations) (December 2018)

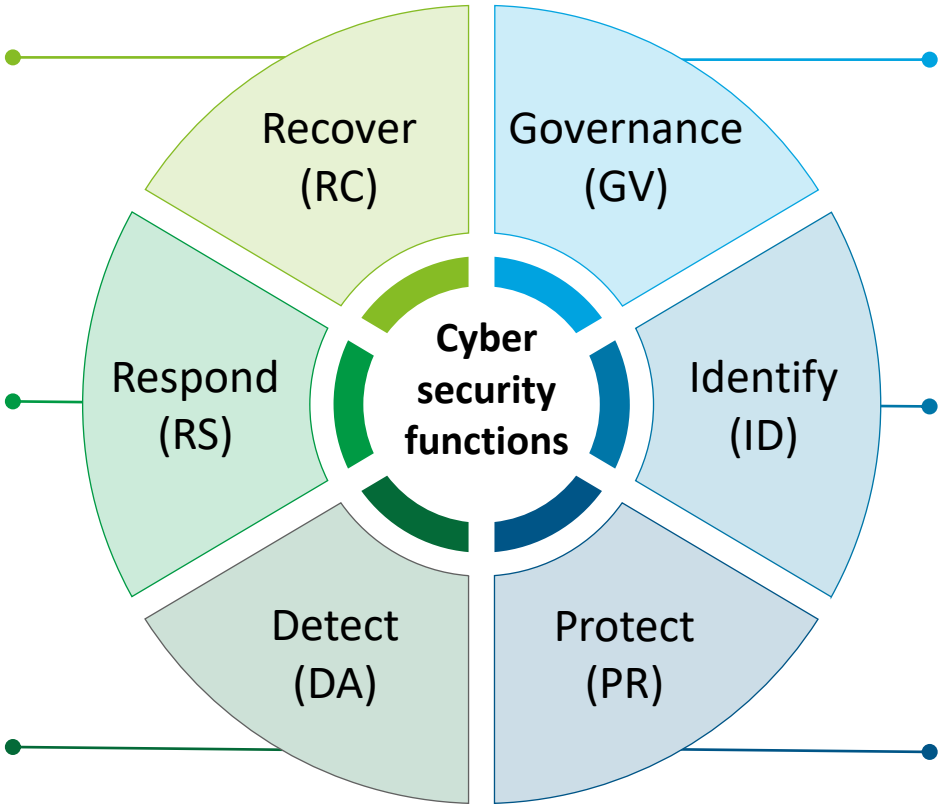
CSCRF: Cybersecurity functions

The framework is broadly based on two approaches: Cybersecurity and Cyber Resilience. The cybersecurity approach covers governance measures to operational controls, and the cyber resilience goals include Anticipate, Withstand, Contain, Recover and Evolve. The framework provides a standardised approach to implementing various cybersecurity and cyber resilience methodologies. Standards such as ISO 27000 series, CIS v8, NIST 800-53, BIS Financial Stability Institute and CPMI-IOSCO guidelines were referred to while formulating this framework.

- RC.RP: Incident recovery plan execution
- RC.CO: Incident recovery communication
- RC.IM: Improvements

- RS.MA: Incident management
- RS.CO: Incident management reporting and communication
- RS.AN: Incident analysis
- RS.IM: Improvements

- DA.CM: Security continuous monitoring
- DA.DP: Detection process



- GV.OC: Organisational context
- GV.RR: Roles, responsibilities and authorities
- GV.PO: Policy
- GV.OV: Oversight
- GV.RM: Risk management
- GV.SC: Supply chain risk management

- ID.AM: Asset management
- ID.RA: Risk assessment

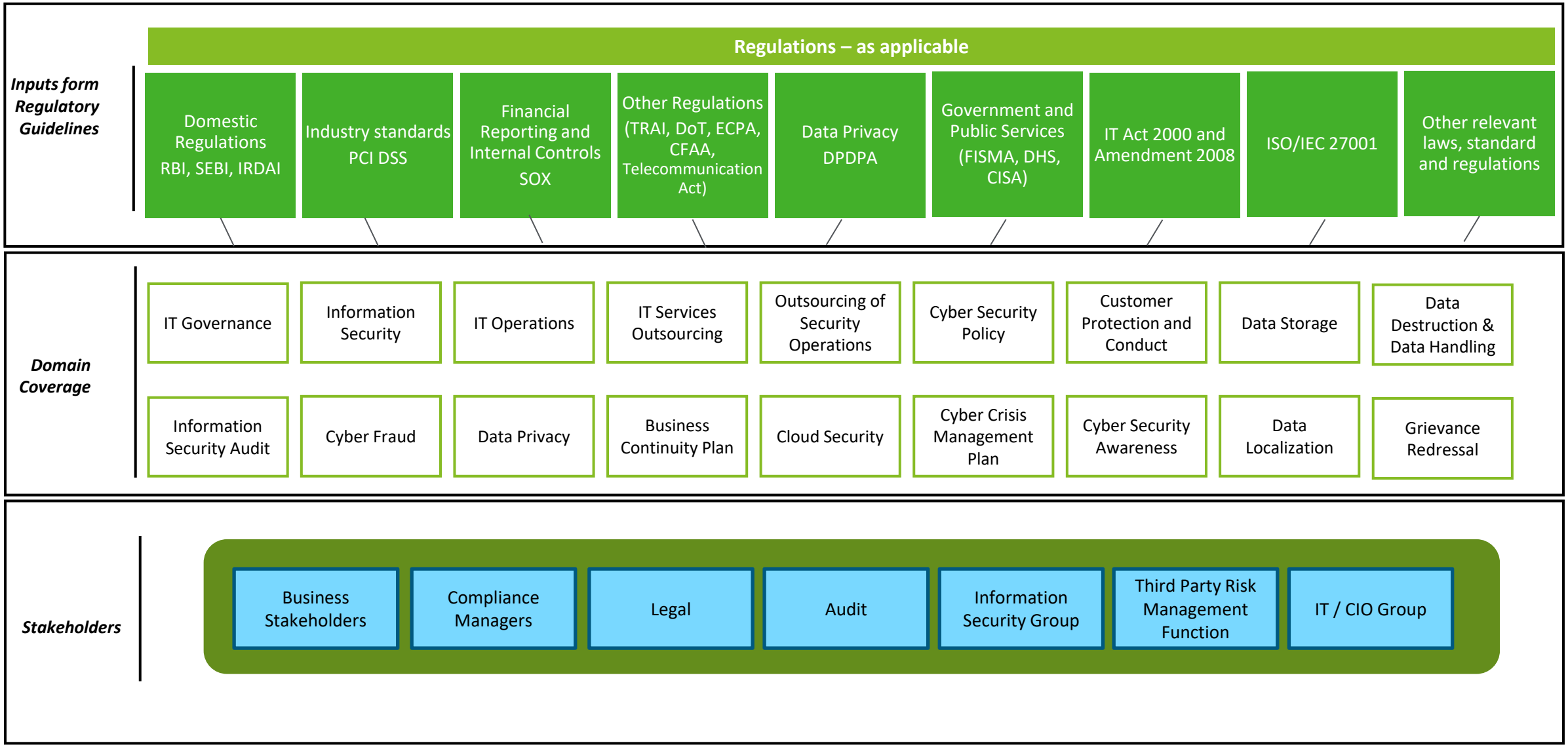
- PR.AA: Identity management, authentication and access control
- PR.AT: Awareness and training
- PR.DS: Data security
- PR.IP: Information protection process and procedure
- PR.MA: Maintenance

A Strategic Approach

This point of view presents a broad framework for CSCRF implementation. The specific details will differ depending on the size, characteristics and intricacy of the REs

Identify As-Is Assessment	Augment Enhance Cyber Program	Implement Continuous control monitoring	Remediate Continuous improvement	Document Reporting to regulator
• Create a unified control framework based on applicable regulatory requirements and frameworks/baselines adopted by the organisation (e.g., SEBI CSCRF, PCI, NIST, ISO 27001) • Identify the scope's applicability per the unified control framework (Locations, infrastructure, business units, etc.) • Inventorize current activities being performed and map with SEBI CSCRF requirements • Perform the gap assessment per the current state analysis against the SEBI CSCRF guidelines and other regulatory circulars (as applicable) • Identify and evaluate current control effectiveness against the unified framework	• Continue existing controls operations for controls that address CSCRF requirement • Design and select new cybersecurity controls based on identified risks and gaps • Establish security governance and oversight • Create or update security policies, procedures or guidelines to align with organisational goals and a unified control framework • Implement the controls and strengthen data protection measures (such as IAM, incident response, DLP, IPS/IDS and EDR) • Improve security monitoring and strengthen incident response and management through SOC services or M-SOC (Market SOC) • Ensure that newly incorporated controls comply with relevant regulations and standards	• Continuous Controls Monitoring (CCM) - Conduct regular compliance checks and audits to verify operational effectiveness of controls framework • Perform thorough testing of new controls to ensure they work as intended • Tailor training content to the specific needs and responsibilities of identified different organisational roles • Plan and schedule regular training sessions to ensure all employees can participate, including new hires and those needing refresher training	• Establish a process for continuously evaluating and improving cybersecurity controls based on CCM • Track the effectiveness of the corrective actions • Continuously monitor compliance with reporting requirements and address any issues or discrepancies • Gathering feedback from stakeholders involved in or affected by the corrective actions • Incorporate successful corrective actions into Standard Operating Procedures (SOPs) or company policies • Regularly reviewing the corrective actions and their outcomes to ensure they remain effective	• Create an annual calendar for the submission of the reports per the frequency specified in SEBI CSCRF reporting requirements • Use the standardised formats of reporting provided by the SEBI CSCRF circular • Set up processes for reviewing and validating report content to ensure accuracy and compliance with the reporting requirements of SEBI CSCRF • Align the assessments / governance / monitoring activities according to the reporting requirements • Gather feedback from stakeholders on the reporting process and content to make necessary adjustments • Prepare and present reports to internal stakeholders, including management and the board • Submit required reports to SEBI per reporting requirements

Deloitte’s Unified Regulatory Compliance Framework for Financial Services



Deloitte.

Sathish Gopalaiah
President, T&T, Deloitte India
sathishtg@deloitte.com

Deepa Seshadri
Partner & Leader – Cyber,
Deloitte South Asia
deseshadri@deloitte.com

Gaurav Shukla
Partner, Deloitte India
shuklagaurav@deloitte.com

Munjal Kamdar
Partner, Deloitte India
mkamdar@deloitte.com

Jignesh Oza
Partner, Deloitte India
jigneshoza@deloitte.com

Ashish Sharma
Partner, Deloitte India
sashish@deloitte.com

Himanshu Surange
Partner, Deloitte
hsurange@deloitte.com

Vikas Garg
Partner, Deloitte India
vikasgarg@deloitte.com

Digvijay Chudasama
Partner, Deloitte India
dchudasama@deloitte.com

Sahil Tagra
Partner, Deloitte India
stagra@deloitte.com

Bhavesh Bhurat
Partner, Deloitte India
bhaveshbhurat@deloitte.com

Sabarinath Madhumohan
Partner, Deloitte India
smadhumohan@deloitte.com

Sowmya Vedarth
Partner, Deloitte India
sovedarth@deloitte.com

Gaurav Khera
Partner, Deloitte India
gkhera@deloitte.com

Aniket Likhite
Executive Director, Deloitte India
alikhite@deloitte.com

Dr. Vikram Venkateswaran
Partner, Deloitte India
vikramv@deloitte.com

Sanbir Keer
Executive Director, Deloitte India
skeer@deloitte.com