Deloitte.

SEBI Circular on Cyber Security and Resilience Framework for Mutual Funds and AMCs

A Point of View

For Private Circulation Only

January 2019

Risk Advisory

Key provisions and highlights of the cyber security and resilience framework*

These guidelines by large can be mapped to the NIST framework. The framework was developed with a focus on industries vital to national and economic security, including energy, banking, communications and the defense industrial base.

The 56 provisions made in the guideline has been mapped to the framework to reflect completeness and comprehensiveness of the circular. The following outlines the key provisions for consideration

Identify and Protect

- Governance
- Identification of critical assets
- Access Controls
- Physical Security
- Network Security Management
- Security of data
- Hardening of hardware and software
- Application security and testing
- Patch management
- Disposal of systems
- Vulnerability Assessment and Penetration Testing

Detect and Respond

- Process for Monitoring
- Implications of internal and external parties
- Detection of attacks on systems & network
- Alerts and respond to unauthorized or abnormal systems

Remediate and Recover

- Timely restoration of systems in line with predefined objectives
- Incident of loss or destruction to be included as ongoing learnings
- Periodic drills, trainings & audits
- Information sharing & transparency

*Refer to the SEBI guidelines provided under the Circular on cyber security and cyber resilience.

Overall Approach

	Current State Assessment (CSA) against SEBI's Guidelines	**Institution of Cyber Security Framework & resilience plan**	**Implementation & Enhancing capability maturity**	**Sustenance & Continuity**
Delivertables	Current State Assessment Report	Cyber Security and Cyber Resilience Framework	Cyber Security and Resilience implementation road map and program charter	Program charter and review reports
Project management	Manage project and communications			

Inputs

Identify and Protect

- ISO[1] 27001/2
- NIST[2] cybersecurity framework
- Global privacy and data protection laws
- ITIL[3]

Leading practices

- Recognized information security leader
- Project/engagement experience
- Published industry research

Threat Landscape

- Who might attack?
- What are they after?
- What tactics will they use?

[1] International Organization for Standardization
[2] National Institute for Standards and Technology
[3] Formerly known as the Information Technology Infrastructure Library

Cyber Risk Framework

Deloitte's Cyber Capability Framework is organized by key capability areas that cover leading industry standards. These capability areas are derived based on our experience serving clients, industry leading practices and applicable regulatory requirements.

Deloitte's Cyber Risk Framework

Business Objectives

Secure	Vigilant	Resilient
Enhance risk-priotized controls to protect against known & emerging threats, & comply with industry cyber security standards & regulations	Detect violations & anomalies through better situational awareness across the environment	Establish the ability to quickly return to normal operations & repair damage to the business

Operating Model Componenets

Actionable threat intelligence		Strategic organizational approach		
Growth / Innovation	**Operational Efficiency**	**Brand Protection**	**Risk-based Decision Making**	**Compliance**
Governance & Oversight The organizational structure, committees, and roles & responsibilities for managing information security	**Policies & Standards** Expectations for the management of information security	**Management Processes** Processes to manage risks in information security risk management and oversight	**Tools & Technology** Tools and technology that support the risk management lifecycle and integration of risk with cyber risk	**Risk Metrics & Dashboard** Reports identifying risks and performance across information security domains; communicated to

Cyber Risk Domains

Secure		Vigilant	Resilient
1. Risk & Compliance Management	5. App Security & Secure SDLC	9. Vulnerability Management	15. Crisis Management
2. Identity & Access Management	6. Asset Management	10. Threat Intelligence	16. Resiliency & Recovery
3. Data Protection & Management	7. Third Party Risk Management	11. Security and Threat Monitoring	17. Cyber Simulations
4. Infrastructure Security	8. Physical Security	12. Cybersecurity Operations	18. Incident Response & Forensics
		13. Predictive Cyber Analytics	
		14. Insider Threat Monitoring	

Business Security

Secure Client Service Delivery

Circular on cyber security and cyber resilience

SEBI

What are these guidelines?

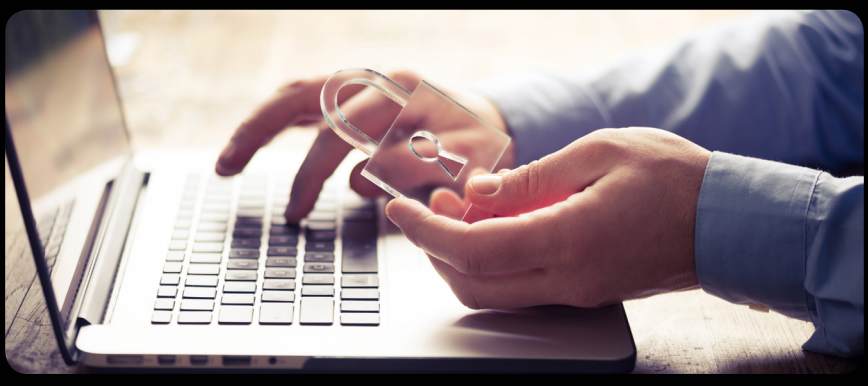
SEBI has issued a circular to maintain robust cyber security and resilience frameworks to protect the integrity of data and breaches against privacy. As part of the operational risk management there is a requirement for all Mutual Funds (MF) and Asset management Companies (AMC) to comply with circular SEBI/HO/IMD/DF2/CIR/P/2019/12 effective April 1 2019

What do these guidelines cover?

The focus of the circular is on Cyber Security and Cyber resilience. It is based on the recommendation of SEBI's High Powered Steering Committee where it was decided that the framework prescribed vide SEBI circular CIR/MRD/DP13/2015 dated July 06, 2015 on cyber security and cyber resilience also be made applicable to all Mutual Funds / Asset Management Companies.

Who are these applicable to?

This guidelines document is applicable to all Mutual Funds and Asset Management Companies regulated by the Securities Exchange Board of India. These guidelines are applicable to all data created, received or maintained by MFs and AMCs wherever these data records are and whatever form they are in, in the course of carrying out their designated duties and functions.



Key contacts

Shree Parthasarathy
Partner
sparthasarathy@deloitte.com

Abhijit Katkar
Partner
akatkar@deloitte.com

Munjal Kamdar
Partner
mkamdar@deloitte.com

George Ittyerah
Director
gittyerah@deloitte.com

Vishal Jain
Partner
jainvishal@deloitte.com

Deloitte.