ManageEngine
Endpoint Central

How Endpoint Central helps you meet RBI's IT GRC directives

With the intent of regulating commercial banks, non-banking financial corporations, credit information companies, and all India financial institutions (AIFIs), the RBI has recently released a directive titled, **Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023.**

These master directions will come into effect from April 1, 2024.

Ok. **Let's break it down for you.** What is the scope of this directive?

The document intends to aid, advise, and provide directions to the banks in the areas of:

01 IT governance

02 Risk, controls, and assurance practices

03 Business continuity/disaster recovery management

What are the **key things that you should note from this directive?**

All the regulated entities must have:

- A robust IT governance framework
- An information security risk management framework
- Cybersecurity policy and cyber crisis management plan
- An IT strategy committee that convenes on a quarterly basis
- An IT steering committee to execute the recommendations and suggestions of the IT strategy committee.

Endpoints form the significant bulk of your IT environment, and it is quintessential to manage and secure them. Banks and other financial institutions tend to have a multitude of OSs and devices. However, their expanding footprint also leads to the heightened probability of cyberattacks. IT experts call this expanding endpoint fleet, which is prone to cyberattacks, the attack surface.

Note:

1. *The master directive has **seven chapters and 32 sections** in total. In this e-book, we specifically explain how Endpoint Central, ManageEngine's unified endpoint management and security offering, could **help you** achieve compliance for **13 sections out of the 32 listed.***

2. *We have mapped the content from RBI IT GRC directives with our features and capabilities for your convienience in understading this document*
   The texts from RBI IT GRC directives will be in italics.

3. *Note 2: Regulated Entities (RE) include commercial banks, non-banking financial corporations, credit information companies, and AIFIs.*

9/32

IT Services Management

"For seamless continuity of business operations, REs shall avoid using outdated and unsupported hardware or software and shall monitor software's end-of-support (EOS) date and Annual Maintenance Contract (AMC) dates of IT hardware on an ongoing basis."

How Endpoint Central helps

- Endpoint Central can help you track high-risk software such as outdated software, peer-to-peer software, unsecure remote sharing software, and eliminate them.
- You can leverage Endpoint Central's warranty management system, which provides you with reports on hardware with soon-to-expire warranty, expired warranty, etc. so that you stay on your toes, managing them.
- Endpoint Central also integrates seamlessly with popular ITSM tools like ManageEngine Servicedesk Plus, Jira Service Management, ServiceNow, Spiceworks, Freshservice, and Zendesk.

11/32

Capacity Management

"On an annual or more frequent basis, REs shall proactively assess capacity requirement of IT resources. REs shall ensure that IT capacity planning across components, services, system resources, supporting infrastructure is consistent with past trends (peak usage), the current business requirements and projected future needs as per the IT strategy of the RE"

How Endpoint Central helps

- With Endpoint Central, admins can analyze software usage duration and the number of times the software is used. With these insights, they can make informed decisions on software purchases while also determining peak usage trends in their IT.
- Endpoint Central has a license management feature to assess if you have adequate software licenses for your users.
- Also, it allows the admins to keep a tab on soon-to-expire and expired software licenses.

13/32

Change & Patch Management

"REs shall put in place documented policy(ies) and procedures for change and patch management to ensure the following:

(a) the business impact of implementing patches/ changes (or not implementing a particular patch/ change request) are assessed.

(b) the patches/ changes are applied/ implemented and reviewed in a secure and timely manner with necessary approvals.

(c) any changes to an application system or data are justified by genuine business needs and approvals supported by documentation and subjected to a robust change management process

(d) mechanism is established to recover from failed changes/ patch deployment or unexpected results."

How Endpoint Central helps

- Endpoint Central provides comprehensive Patch support for Windows, Linux, and macOSs and Windows Server OS. It also can patch 1,000+ third party applications, hardware drivers, and BIOS.
- Endpoint Central has a vulnerability age matrix and vulnerability severity summary, which can provide rich insights about the impact of patch implementation. Besides, Endpoint Central also provides comprehensive reports on vulnerable systems and missing patches in your IT.
- Endpoint Central also provides for testing and approving patches so that IT admins can test the patches within a small group of computers and later deploy them into your whole organization.
- For multi-level patch approval requirements, Endpoint Central has low code policy orchestration, that helps enterprises build customized patch approval workflows.
- Endpoint Central provides for uninstall patches if the patch deployment doesn't give desired/unexpected results.

Audit Trails

"a) Every IT application which can access or affect critical or sensitive information shall have necessary audit and system logging capability and should provide audit trails.

(b) The audit trails shall satisfy a RE's business requirements apart from regulatory and legal requirements. The audit trails must be detailed enough to facilitate the conduct of audit, serve as forensic evidence when required, and assist in dispute resolution, including for non-repudiation purposes.

(c) REs shall put in place a system for regularly monitoring the audit trails and system logs to detect any unauthorized activity."

How Endpoint Central helps

- Endpoint Central has comprehensive reporting capability. Apart from providing deep insights about endpoint estate, it can also be used for governance and auditing purposes.
- For auditing critical computers having sensitive applications, User Logon reports can help admins track users' access to critical endpoints.
- Endpoint Central also provides detailed audit reports containing access requests for popular blacklisted applications.
- A DPO Dashboard has rich insights on Bitlocker status, vulnerable system status, firewall status, and much more.
- The super admin of the Endpoint Central console can receive notifications when the IT technicians working on Endpoint Central reset their passwords, when their accounts get disabled due to multiple login failures, or when a new technician account is created or deleted.
- Under the personalization setting in the Endpoint Central console, the admins can view the concurrent sessions of users logged into the Endpoint Central console and use the same for audit trials.
- Endpoint Central's remote screen sharing feature allows the technicians to record the screen sharing sessions, which are useful for audit trials and knowledge transfer.

16/32

Cryptographic controls

"The key length, algorithms, cipher suites and applicable protocols used in transmission channels, processing of data and authentication purpose shall be strong. REs shall adopt internationally accepted and published standards that are not deprecated/ demonstrated to be insecure/ vulnerable and the configurations involved in implementing such controls shall be compliant with extant laws and regulatory instructions"

How Endpoint Central helps

- Endpoint Central uses FIPS 140-2 compliant algorithms. Users can enable FIPS mode to run their IT on a highly secure environment.

19/32

Access Controls

(a) Access to information assets shall be allowed only where a valid business need exists. REs shall have documented standards and procedures, which are approved by the ITSC and kept up to date for administering need-based access to an information system.

(b) Personnel with elevated system access entitlements shall be closely supervised with all their systems activities logged and periodically reviewed.

(c) REs shall adopt multi-factor authentication for privileged users of i) critical information systems and ii) for critical activities, basis the RE's risk assessment.

How Endpoint Central helps

- Endpoint Central leverages the principle of least privilege and has a robust endpoint privilege management capability, providing for application specific privilege management and just-in-time access to the end users.
- It has conditional access policies to validate authorized users to access business critical systems and data.
- For IT admins and security ops to access the Endpoint Central console, Endpoint Central provides with role based access control and MFA.

Controls on Teleworking

In the teleworking environment, REs, inter alia, shall:

(a) Ensure that the systems used and the remote access from alternate work location to the environment hosting RE's information assets are secure;

(b) Implement multi-factor authentication for enterprise access (logical) to critical systems;

(c) Put in place a mechanism to identify all remote-access devices attached/ connected to the RE's systems;

(d) Ensure that data/ information shared/ presented in teleworking is secured appropriately

How Endpoint Central helps

- Endpoint Central has secure, HIPAA compliant remote desktop troubleshooting feature (Windows, Mac, and Linux) through which admins can perform remote screen sharing and allows admins to troubleshoot endpoints by accessing end user's Windows system tools, command prompts, and powershell, without the need of screen sharing.
- Endpoint Central's dashboards provide a holistic view about systems connected to the Endpoint Central server, available for remote troubleshooting.
- Endpoint Central's remote screen sharing feature allows the technicians to record the screen sharing sessions, which are useful for audit trials and knowledge transfer.

Metrics

"(a) REs shall define suitable metrics for system performance, recovery and business resumption, including Recovery Point Objective (RPO) and Recovery Time Objective (RTO), for all critical information systems.

(b) For non-critical information systems, REs shall adopt a risk-based approach to define suitable metrics.

(c) REs shall implement suitable scorecard/ metrics/ methodology to measure IT performance and IT maturity level."

How Endpoint Central helps

- Endpoint Central has a vulnerability age matrix and vulnerability severity summary. It also provides comprehensive reports on vulnerable systems and missing patches in your network.
- For both critical and non-critical information systems, Endpoint Central provides for risk-based vulnerability management so that admins can prioritize the vulnerabilities based on metrics like CVSS score, patch availability, and much more.
- Endpoint Central provides Endpoint Analytics. The Endpoint Central server collects telemetry data from endpoints, which comprises disk space, CPU usage, memory usage, warranty, device age, application performance, and more.
- The devices are assigned a baseline score. If any of the devices are found breaching the baseline scores, Endpoint Central will suggest suitable actions to resolve the issues.

25/32

Risk Assessment

"(a) The risk assessment for each information asset within the RE's scope shall be guided by appropriate security standards/ IT control frameworks.

(b) REs shall ensure that all staff members and service providers comply with the extant information security and acceptable-use policies as applicable to them.

(c) REs shall review their security infrastructure and security policies at least annually, factoring in their own experiences and emerging threats and risks. REs shall take steps to adequately tackle cyber-attacks including phishing, spoofing attacks and mitigate their adverse effects."

How Endpoint Central helps

- Endpoint Central can help you track high-risk software such as outdated software, peer-to-peer software, unsecure remote sharing software, and eliminate them.
- Endpoint Central has provisions to distribute terms of use policies to users that can contain security mandates, compliances, and recommendations. It allows admins to inform the users about the data collected from their devices and the reasons for the same.

26/32

Conduct of Vulnerability Assessment (VA) / Penetration Testing (PT)

"(a) For critical information systems and/ or those in the De-Militarized Zone (DMZ) having customer interface, VA shall be conducted at least once in every six months and PT at least once in 12 months. Also, REs shall conduct VA/ PT of such information systems throughout their lifecycle (pre-implementation, post implementation, after major changes, etc.).

(b) For non-critical information systems, a risk-based approach shall be adopted to decide the requirement and periodicity of conduct of VA/ PT.

(c) VA/ PT shall be conducted by appropriately trained and independent information security experts/ auditors.

(d) In the post implementation (of IT project/ system upgrade, etc.) scenario, the VA/ PT shall be performed on the production environment. Under unavoidable circumstances, if the PT is conducted in test environment, REs shall ensure that the version and configuration of the test environment resembles the production environment. Any deviation should be documented and approved by the ISC.

(e) REs shall ensure to fix the identified vulnerabilities and associated risks in a timebound manner by undertaking requisite corrective measures and ensurethat the compliance is sustained to avoid recurrence of known vulnerabilities such as those available in Common Vulnerabilities and Exposures (CVE) database.

(f) REs shall put in place a documented approach for conduct of VA/ PT covering the scope, coverage, vulnerability scoring mechanism (e.g., Common Vulnerability Scoring System) and all other aspects. This may also apply to the RE's information systems hosted in a cloud environment."

How Endpoint Central helps

- Endpoint Central provides comprehensive vulnerability management in terms of constant assessment and visibility of threats from a single console. Apart from vulnerability assessment, it also provides built-in remediation of the vulnerabilities detected.
- For both critical and non-critical information systems, Endpoint Central provides risk-based vulnerability management so that admins can prioritize the vulnerabilities based on metrics like CVSS score, CVE impact type, Patch availability, and much more.
- Endpoint Central provides a unified console for ITOps and SecOps to manage and secure endpoints. Endpoint Central has role based access control so that security functions of the IT can be assigned to independent security experts.

Cyber Incident Response and Recovery Management

"(a) The cyber incident response and recovery management policy shall address the classification and assessment of incidents; include a clear communication strategy and plan to manage such incidents, contain exposures and achieve timely recovery.

(b) REs shall analyse cyber incidents (including through forensic analysis, if necessary) for their severity, impact and root cause. REs shall take measures, corrective and preventive, to mitigate the adverse impact of incidents on business operations.

(c) REs shall have written incident response and recovery procedures including identification of key roles of staff/ outsourced staff handling such incidents.

(d) REs shall have clear communication plans for escalation and reporting the incidents to the Board and Senior Management as well as to customers, as required. REs shall pro-actively notify CERT-In and RBI17 regarding incidents, as per regulatory requirements. REs are also encouraged to report the incidents to Indian Banks – Centre for Analysis of Risks and Threats (IB-CART) set up by IDRBT.

(e) REs shall establish processes to improve incident response and recovery activities and capabilities through lessons learnt from past incidents as well as from the conduct of tests and drills. REs, inter alia, shall ensure effectiveness of crisis communication plan/ process by conduct of periodic drills/ testing with stakeholders (including service providers)."

How Endpoint Central helps

- Endpoint Central has a built-in next gen antivirus engine (currently available as early access) that proactively detects cyberthreats with its AI-assisted, real-time behavior detection and deep learning technology.
- Apart from real-time threat detection, Endpoint Central also actively performs incident forensics so that SecOps analyze the root cause and severity of the threats.
- If the next gen antivirus engine detects a suspicious behavior in endpoints, it can quarantine those endpoints and, after a thorough forensic analysis, can be deployed back into production.

- Endpoint Central also provides instant, non-erasable backup of the files in your network every three hours by leveraging Microsoft's volume shadow copy service.
- If a file is infected with ransomware, it can be restored with the most recent backup copy of the file.

28/32

Business Continuity Plan (BCP) and Disaster Recovery (DR) Policy

"(a) The BCP and DR policy shall adopt best practices to guide its actions in reducing the likelihood or impact of the disruptive incidents and maintaining business continuity. The policy shall be updated based on major developments/ risk assessment.

(b) RE's BCP/ DR capabilities shall be designed to effectively support its resilience objectives and enable it to rapidly recover and securely resume its critical operations (including security controls) post cyber-attacks/ other incidents."

How Endpoint Central helps

- Endpoint Central can quarantine endpoints that exhibit suspicious behavior and, after a thorough forensic analysis, can be deployed back into production.
- Endpoint Central also provides instant, non-erasable backup of the files in your network every three hours by leveraging Microsoft's volume shadow copy service.
- If a file is infected with ransomware, it can be restored with the most recent backup copy of the file.

30/32

Information Systems (IS) Audit

(a) The Audit Committee of the Board (ACB) shall be responsible for exercising oversight of IS Audit of the RE.

(b) REs shall put in place an IS Audit Policy. The IS Audit Policy shall contain a clear description of its mandate, purpose, authority, audit universe, periodicity of audit etc. The policy shall be approved by the ACB and reviewed at least annually.

(c) The ACB shall review critical issues highlighted related to IT / information security / cyber security and provide appropriate direction and guidance to the RE's Management.

(d) REs shall have a separate IS Audit function or resources who possess required professional skills and competence within the Internal Audit function. Where the RE uses external resources for conducting IS audit in areas where skills are lacking within the RE, the responsibility and accountability for such external IS audits would continue to remain with the competent authority within Internal Audit function.

(e) REs shall carry out IS Audit planning by adopting a risk-based audit approach.

(f) REs may consider, wherever possible, a continuous auditing approach for critical systems, performing control and risk assessments on a more frequent basis.

How Endpoint Central helps

Endpoint Central is designed to meet governance, risk, and compliances (GRC) requirements of the enterprises. Endpoint Central's powerful reporting capabilities can be used for auditing purposes.

Reference: Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023