SYBER GRC

Are You in Compliance?

RBI/2019-20/129 - Reserve Bank of India: Comprehensive Cybersecurity Framework for Primary (Urban) Cooperative Banks (UCBs)

Outlined below are some key takeaways from The Reserve Bank of India's cyber security controls for primary (urban) cooperative banks (UCBs); and ways SyberGRC can assist in achieving compliance.

Level II - Annex II - 2. Secure Configuration (2.1)

Document and apply baseline security requirements/configurations to all categories of devices (end-points/workstations, mobile devices, operating systems, databases, applications, network devices, security devices, security systems, etc.), throughout the lifecycle (from conception to deployment) and carry out reviews periodically.

How We Help:

SyberGRC and iDPS can provide the **location of sensitive data across all assets** that your organization manages. This bird's eye view of your data allows for the adequate oversight of all end-points and devices that host valuable information.

Level II - Annex II - 6. User Access Control / Management (6.1)

Provide secure access to the UCB's assets/services from within/outside UCB's network by protecting data/information at rest (e.g. using encryption, if supported by the device) and in-transit (e.g. using technologies such as VPN or other standard secure protocols, etc.)

How We Help:

Compliance with this measure requires the knowledge of all static data your organization holds. iDPS data discovery scans will **identify files that already contain permissions** and can help bifurcate sensitive data that is already encrypted vs. data still requiring protection. .

Level III - Annex III - 6. Maintenance, Monitoring, and Analysis of Audit Logs (6.2)

Manage and analyse audit logs in a systematic manner so as to detect, respond, understand or recover from an attack.

How We Help:

iDPS scans classify, identify, and locate all sensitive data across your business using **customized keywords that are critical to your operations and industry**. This mission critical data is what can be assessed and monitored before, during, and after incidents.

Level III - Annex III - 7. Incident Response and Management (7.2)

UCBs shall have necessary arrangements, including a documented procedure, with such third party vendors/service providers for such purpose. This shall include, among other things, to get informed about any cyber security incident occurring in respect of the bank on timely basis to early mitigate the risk as well as to meet extant regulatory requirements.

How We Help:

iDPS uses proprietary, patented technology to **derive the monetary value of each static file it identifies**. This analysis can serve as a benchmark for decision making, in regards to incident disclosure.

Level IV - Annex IV - 4. Forensics and Metrics (4.1)

Develop a comprehensive set of metrics that provides for prospective and retrospective measures, like key performance indicators and key risk indicators. Some illustrative metrics include coverage of anti-malware software...vulnerability related metrics, number of open vulnerabilities, IS/security audit observations, etc.

How We Help:

iDPS **provides a comprehensive report of static data** your organization is looking to protect. This overview of files and assets is an ideal tool for any forensic analysis being performed on a system, and should absolutely satisfy compliance to this measure.

Contact Us

https://www.sybergrc.com