HCLSoftware

HCL **BigFix** Support of RBI Requirements

HCL BigFix

The Reserve Bank of India (RBI) has issued a Cybersecurity Framework that mandates all commercial banks in India to establish robust policies and adopt advanced technologies to address growing security threats. Similar to other security frameworks like ISO 27001 or CIS Security Controls, the RBI Cybersecurity Framework outlines a set of Baseline Controls that banks must implement.

HCL BigFix is a powerful solution widely used by financial institutions to comply with security regulations and implement frameworks effectively. BigFix addresses critical RBI Baseline Control requirements, including device inventory, secure configuration, unauthorized software prevention, and patch/vulnerability management.
This document outlines how BigFix supports various RBI Baseline Control requirements to help banks achieve continuous security and compliance.

HCL BigFix

RBI Cybersecurity Framework Baseline Controls	Support by HCL BigFix
1 Inventory Management of Business IT Assets	
1.1 Maintain an up-to-date inventory of Assets, including business data/information including customer data / information, business applications, supporting IT infrastructure and facilities – hardware / software / network devices, key personnel, services, etc. indicating their business criticality. The banks may have their own framework / criteria for identifying critical assets.	**HCL BigFix Asset Discovery**: Automatically finds all devices with an IP address on the network using NMAP scanning, creating a full inventory of hardware assets. **HCL BigFix Inventory:** Centralized inventory showing detailed hardware specifications, installed software, and license usage.
2 Preventing execution of unauthorized software	
2.1 Maintain an up-to-date and preferably centralized inventory of authorized / unauthorized software(s). Consider implementing whitelisting of authorized applications / software/libraries, etc.	**Control Software**: HCL BigFix Inventory offers a centralized, detailed inventory of installed software, including vendor version, utilization rates, allowlist, block list and end-of-life date. It ensures only authorized software is on all devices, swiftly identifying and removing unauthorized applications.
2.2 Have a mechanism to centrally / otherwise control installation of software / applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. and a mechanism to block / prevent and identify installation and running of unauthorized software / applications on such devices / systems.	**Automated Software Management**: HCL BigFix Lifecycle Software Distribution enables seamless software management across all devices, ensuring control, automation, and software compliance. With policy-based deployment, closed-loop verification, and a self-service app, it guarantees software integrity and security. **Centralized Software Compliance**: HCL BigFix Inventory provides a centralized, detailed inventory of installed software across all devices, enabling the detection and removal of unauthorized software that may contain vulnerabilities or malware, ensuring robust software compliance.
2.3 Continuously monitor the release of patches by various vendors / OEMs, advisories issued by CERT-in and other similar agencies and expeditiously apply the security patches as per the patch management policy of the bank. If a patch/series of patches is/are released by the OEM / manufacturer / vendor for protection against well-known / well publicized / reported attacks exploiting the vulnerability patched, the banks must have a mechanism to apply them expeditiously following an emergency patch management process.	**Rapid Patching**: HCL BigFix Patch delivers out-of-the-box patching for various OS platforms like Windows, UNIX, Linux, macOS, and common third-party applications, ensuring timely updates. Rigorous application of security patches is the most effective method for vulnerability management. **Seamless Remediation**: HCL BigFix Insights for Vulnerability Remediation integrates with Tenable, Qualys, Rapid7, and has a .csv ingestion mechanism to correlate their data with BigFix contents. This guides users on applying the best patch and configuration settings, enhancing vulnerability management, and reducing security risks efficiently.
2.4 Have a clearly defined framework including requirements justifying the exception(s), duration of exception(s), process of granting exceptions, and authority for approving, authority for review of exceptions granted on a periodic basis by officer(s) preferably at senior levels who are well equipped to understand the business and technical context of the exception(s).	**Exception Management**: HCL BigFix Compliance provides an exception management feature that excludes devices from compliance reports, specifying business reasons, affected devices, and expiration dates. It also maintains a detailed exception history for full transparency.

HCL BigFix

RBI Cybersecurity Framework Baseline Controls	Support by HCL BigFix
4 Network Management and Securit	
4.2 Maintain an up-to-date / centralized inventory of authorized devices connected to the bank's network (within / outside bank's premises) and authorized devices enabling the bank's network. The bank may consider implementing solutions to automate network discovery and management.	**Complete Asset Discovery**: HCL BigFix Asset Discovery uses distributed NMAP scanning to detect devices on the network with an IP address.BigFix can report on devices that are managed by BigFix and can report on properties including networking information, that can then be used for various automation and policy enforcement strategies.
4.3 Ensure that all the network devices are configured appropriately and periodically assess whether the configurations are appropriate to the desired level of network security.	**Continuous Compliance Assessment**: BigFix Compliance ensures device configurations meet CIS benchmarks, DISA STIGs, and PCI Compliance. **Network Access Control**: BigFix integrates with Network Access Control (NAC) solutions to check a device's status, such as the presence of a BigFix Agent or compliance with patch and configuration policies, to authorize network access, ensuring robust security compliance.
4.4 Put in appropriate controls to secure wireless local area networks, wireless access points, wireless client access systems.	**Wireless Security Compliance**: HCL BigFix Compliance assesses and remediates security configuration controls for wireless access, supporting CIS benchmarks or DISA STIGs. **Policy-Based Wireless Management**: HCL BigFix provides general device management capabilities, allowing the establishment of dynamic policies for individual devices' use of wireless network adapters based on location and other variables. **Network Access Control Integration**: HCL BigFix integrates with Network Access Control (NAC) solutions to verify a device's status and authorize access to wireless networks, ensuring comprehensive security compliance.
4.5 Have mechanisms to identify authorized hardware / mobile devices like Laptops, mobile phones, tablets, etc. and ensure that they are provided connectivity only when they meet the security requirements prescribed by the bank.	**Comprehensive Endpoint Management**: HCL BigFix manages a wide variety of endpoints, including servers, desktops, laptops, kiosks, ATMs, and mobile devices. BigFix Compliance ensures network security by assessing and remediating configurations according to CIS benchmarks and DISA STIGs, ensuring robust security compliance.
4.6 Have a mechanism to automatically identify unauthorized device connections to the bank's network and block such connections.	**Network Access Control Integration**: HCL BigFix integrates with Network Access Control (NAC) solutions to check a device's status, such as the presence of a BigFix Agent or compliance with patch and configuration policies, to authorize network access, ensuring robust security compliance.
4.7 Put in place a mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints.	**Real-Time Threat Detection**: BigFix agents run on each managed system, monitoring and detecting unusual activities that could indicate a security incident. Detected anomalies can trigger remediation actions, such as quarantining the system, and enhancing threat intelligence and security.

HCL BigFix

RBI Cybersecurity Framework Baseline Controls	Support by HCL BigFix
5 Secure Configuration	
5.1 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.	**Comprehensive Security Compliance**: HCL BigFix Compliance offers tools to create and enforce baseline security policies based on CIS, DISA, and PCI DSS benchmarks for various endpoints, including servers, desktops, laptops, OS, and other applications. It continuously assesses and remediates compliance status against these policies, ensuring robust security compliance. **Mobile Device Management**: BigFix Mobile provides hundreds of out-of-the-box policies and commands, such as passcode settings, restrictions policies, application blacklisting/whitelisting, and remote lock/wipe/restart, to effectively manage and secure mobile devices, protecting business information.
5.2 Periodically evaluate critical device (such as firewall, network switches, security devices, etc.) configurations and patch levels for all systems in the bank's network including in Data Centers, in third party hosted sites, shared-infrastructure locations.	**Continuous Security and Compliance Evaluation**: HCL BigFix provides powerful tools to continuously evaluate the security configurations and patch levels of all critical systems in data centers, remote branches, offices and third-party locations. It delivers periodic reports to maintain a strong security compliance posture.

HCL BigFix

RBI Cybersecurity Framework Baseline Controls	Support by HCL BigFix
7 Patch / Vulnerability & Change Management	
7.1 Follow a documented risk-based strategy for inventorying IT components that need to be patched, identification of patches and applying patches so as to minimize the number of vulnerable systems and the time window of vulnerability / exposure.	**Comprehensive Patch Management**: HCL BigFix Patch offers tools and out-of-the-box content for various OS platforms including Windows, UNIX, Linux, macOS and many common third party middleware and applications. It identifies systems needing patches, applies them, and reports the status, ensuring effective vulnerability management.
7.2 Put in place systems and processes to identify, track, manage and monitor the status of patches to operating system and application software running at end-user devices directly connected to the Internet and in respect of Server operating Systems/Databases/Applications/ Middleware, etc.	**Streamlined Patch Management**: HCL BigFix Patch offers administrative tools and out-of-the-box patching for various OS platforms, including Windows, UNIX, Linux, macOS, and common third-party middleware and applications. It identifies systems needing patches, applies them, and reports the status, automating and streamlining the patch management and vulnerability management process across all devices and systems.
7.3 Changes to business applications, supporting technology, service components and facilities should be managed using robust configuration management processes, configuration baseline that ensure integrity of any changes thereto.	**Baseline Security Enforcement**: HCL BigFix Compliance provides tools and contents to help an organization create and enforce baseline security policies based on best practice security benchmarks published by CIS, DISA, and PCI DSS for a wide categories of endpoints (server, desktop/laptop, web server, database, browser, etc.) to ensure the integrity of the business systems and applications.
7.6 As a threat mitigation strategy, identify the root cause of the incident and apply necessary patches to plug the vulnerabilities.	**Effective Threat Mitigation**: HCL BigFix Patch addresses vulnerabilities contributing to security incidents with a high first-time patching success rate, ensuring robust threat intelligence. BigFix Insights for Vulnerability Remediation integrates with Tenable, Qualys, and Rapid7 to correlate vulnerability data with BigFix contents, guiding users to apply the best patches to remediate discovered vulnerabilities and significantly reduce security risks, enhancing vulnerability management. **Patch Monitoring and PLA Compliance**: HCL BigFix enables IT Operation teams to report on devices with outstanding patches, including the time elapsed since their release. Additionally, BigFix provides a Patching Level Agreement (PLA) report, allowing teams to set a patching cadence commitment and monitor progress towards achieving that timeframe.

HCL BigFix

RBI Cybersecurity Framework Baseline Controls	Support by HCL BigFix
8 User Access Control / Management	

RBI Cybersecurity Framework Baseline Controls	Support by HCL BigFix
8.3 Disallow administrative rights on end-user workstations/ PCs / laptops and provide access rights on a need to know basis and for specific duration when it is required following an established process.	**Controlled Access Management**: HCL BigFix Compliance provides platform or application-specific checklists, supporting CIS benchmarks or DISA STIGs, to help organizations create and enforce system access policies. This includes disabling administrative accounts on end-user systems and granting access only for specific periods as required ensuring robust security compliancт.
8.6 Implement controls to minimize invalid logon counts, deactivate dormant accounts.	**Minimize Invalid Logon Attempt**: BigFix Compliance provides platform or application-specific checklists, supporting CIS benchmarks or DISA STIGs, to help organizations enforce secure logon policies. This includes locking out a user's account after a number of failed login attempts, minimizing displayed information during logon, and deactivating unused accounts.
8.8 Implement measures to control installation of software on PCs/laptops, etc.	**Software Installation Control**: HCL BigFix Lifecycle Software Distribution offers policy-based software installation, ensuring only authorized applications are installed on PCs/laptops. It uses closed-loop verification and a self-service app to maintain software compliance and integrity.
8.9 IImplement controls for remote management / wiping / locking of mobile devices including laptops, etc.	**Comprehensive Mobile Device Management**: BigFix Mobile offers zero-touch provisioning for fast and simple deployment of new endpoints, providing unparalleled visibility and control to organizations. It delivers hundreds of out-of-the-box policies and commands, such as passcode policies, application restrictions, blacklisting/whitelisting, and remote lock/wipe, ensuring robust security compliance and protection of business information on the mobile devices.

HCL BigFix

RBI Cybersecurity Framework Baseline Controls	Support by HCL BigFix
11 Vendor Risk Management	
11.4 Establish appropriate framework, policies and procedures supported by baseline system security configuration standards to evaluate, assess, approve, review, control and monitor the risks and materiality of all its vendor / outsourcing activities shall be put in place.	**Comprehensive Vendor System Discovery**: BigFix Asset Discovery uses NMAP scanning to identify all networked systems with IP addresses, including those owned by external vendors, as long as a BigFix Agent is installed and is reachable by the BigFix Server. This ensures thorough security compliance and visibility across all vendor systems. **Continuous Compliance Monitoring**: BigFix Compliance enforces baseline security policies based on CIS benchmarks, DISA STIGs, and PCI DSS. It continuously monitors, assesses, and reports the compliance status of all managed devices, ensuring robust security and compliance.

RBI Cybersecurity Framework Baseline Controls	Support by HCL BigFix
12 Removable Media	
12.1 Define and implement policy for restriction and secure use of removable media / BYOD on various types / categories of devices including but not limited to workstations / PCs / Laptops / Mobile devices / servers, etc. and secure erasure of data on such media after use.	**Comprehensive Endpoint Management**: BigFix manages a wide variety of endpoints, including servers, desktops, laptops, kiosks, ATMs, and mobile devices. BigFix Compliance provides platform or application specific checklists, in support of CIS benchmarks or DISA STIGs, to help an organization enforce security policies to restrict the use of removable media on all types of devices. **Mobile Device Management**: BigFix Mobile provides hundreds of out-of-the-box policies and commands, such as passcode settings, restrictions policies, application blacklisting/whitelisting, and remote lock/wipe/restart, to effectively manage and secure mobile devices including BYOD, protecting business information.

HCL BigFix

RBI Cybersecurity Framework Baseline Controls	Support by HCL BigFix
13 Advanced Real-time Threat Defense and Management	
13.2 Implement Anti-malware, Antivirus protection including behavioral detection systems for all categories of devices – (Endpoints such as PCs / laptops / mobile devices etc.), servers (operating systems, databases, applications, etc.), Web / Internet gateways, email-gateways, Wireless networks, SMS servers etc. including tools and processes for centralized management and monitoring.	**Centralized Endpoint Protection**: BigFix Compliance's Client Manager for Endpoint Protection (CMEP) provides real-time visibility and single-point control for managing antivirus and malware protection from vendors like Symantec, McAfee, Trend Micro, Sophos, CA, and Microsoft. The CMEP module monitors and reports if antivirus clients on managed systems are healthy and if virus definitions are up-to-date, ensuring robust security compliance and effective vulnerability management across all devices.

17 Audit Log Settings	
17.1 Implement and periodically validate settings for capturing of appropriate logs/audit trails of each device, system software and application software , ensuring that logs include minimum information to uniquely identify the log for example by including a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or event and/or transaction.	**Ensured Audit Logging**: BigFix Compliance provides platform or application-specific checklists, supporting CIS benchmarks or DISA STIGs, to ensure that system/audit logging settings on endpoints are always enabled and cannot be disabled by users. This guarantees that appropriate logging information, including date, timestamp, source and destination addresses, and other essential data, is always available for collection and analysis, ensuring robust security compliance.

RBI Cybersecurity Framework Baseline Controls	Support by HCL BigFix
18 Vulnerability Assessment and Penetration Test and Red Team Exercises	
18.1 Periodically conduct vulnerability assessment and penetration testing exercises for all the critical systems, particularly those facing the Internet.	**Agent-Based Vulnerability Scanning**: BigFix Compliance provides agent-based vulnerability scanning for Windows systems, based on the standardized Open Vulnerability and Assessment Language (OVAL) security vulnerability definitions published by CIS. **Continuous Compliance Monitoring**: BigFix Compliance enforces baseline security policies based on CIS benchmarks, DISA STIGs, and PCI DSS. It continuously monitors, assesses, and reports the compliance status of all managed devices, ensuring robust security and compliance. **Advanced Threat Reporting**: BigFix CyberFOCUS offers advanced reporting tools, including real-time dashboards that track remediation tasks and align them with business security goals. With integrated threat intelligence and vulnerability scanners, CyberFOCUS prioritizes the most critical risks, providing clear insights into the remediation process and enhancing overall security efforts.
18.2 The vulnerabilities detected are to be remedied promptly in terms of the bank's risk management/treatment framework so as to avoid exploitation of such vulnerabilities.	**Prompt Vulnerability Remediation**: BigFix Patch offers administrative tools and out-of-the-box patching for various OS platforms, including Windows, UNIX, Linux, and macOS. It identifies systems needing patches, applies them, and reports the status. BigFix Insights for Vulnerability Remediation integrates with Tenable and Qualys, correlating their data with BigFix to guide users in applying the best patches and configuration settings, effectively reducing security risks and ensuring robust vulnerability management.

HCLSoftware