HCLSoftware

HCL BigFix Ensuring NCA Compliance

Securing the Future: The Role of NCA in Saudi Arabia's Digital Transformation

HCL **BigFix**

Executive Summary

Saudi Arabia's Vision 2030 sets a bold agenda for national transformation, focusing on enhancing the country's security, economy, and overall well-being. A key element of this vision is the advancement of the Kingdom's digital infrastructure, aiming to keep pace with the global evolution in digital services, interconnected networks, and IT/OT systems. As the country prepares for the 4th Industrial Revolution, including the integration of artificial intelligence and vast data exchanges, ensuring the seamless flow and security of information becomes essential. Organizations play a crucial role in strengthening the Kingdom's overall cybersecurity resilience by ensuring compliance with NCA standards.

Robust cybersecurity measures are vital to safeguard the Kingdom's national security, critical infrastructure, and key sectors. This led to the establishment of the National Cybersecurity Authority (NCA), formalized by Royal Decree 6801, making it the central authority on cybersecurity. The NCA is tasked with developing and enforcing national policies, governance frameworks, and cybersecurity standards. While the NCA provides oversight and guidance, every organization, public or private, is responsible for securing its own networks, systems, and data, as reinforced by Royal Decree 57231.

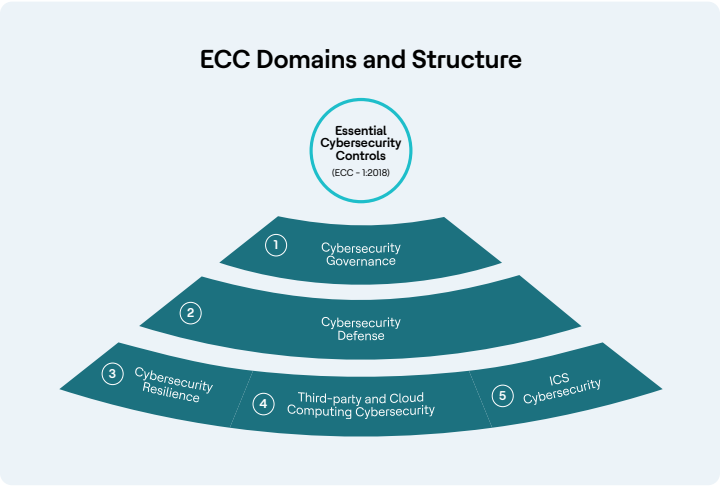
HCL BigFix plays a crucial role in helping organizations meet NCA's stringent cybersecurity requirements. As a unified platform, BigFix provides comprehensive endpoint management, automates compliance enforcement, and enables real-time monitoring to ensure continuous security. This document outlines how BigFix empowers organizations to tackle compliance challenges, streamline patch management, perform vulnerability assessments, and maintain NCA compliance—all while enhancing their overall security posture.

Why NCA's Essential Cybersecurity Controls (ECC) Matter

The National Cybersecurity Authority (NCA) created the Essential Cybersecurity Controls (ECC) to protect Saudi Arabia's critical information and technology assets. After thorough research of global standards, national laws, and past cybersecurity incidents, the ECC framework was designed to address the rising need for stronger cybersecurity across the Kingdom.

The Essential Cybersecurity Controls consist of the following:

- **5 Main Domains:**
  1. Cybersecurity Governance
  2. Cybersecurity Defense
  3. Cybersecurity Resilience
  4. Third-party and Cloud Computing Cybersecurity
  5. Industrial Control Systems (ICS) Cybersecurity
- **29 Subdomains**
- **114 Cybersecurity Controls**



Objective of the Essential Cybersecurity Controls

The Essential Cybersecurity Controls (ECC) aim to establish minimum requirements for protecting an organization's information and technology assets. These requirements focus on:

- **Confidentiality**
- **Integrity**
- **Availability**

These controls are supported by four foundational pillars that ensure a comprehensive approach to cybersecurity:

- **Strategy**
- **People**
- **Processes**
- **Technology**

ECC Scope of Work

The Essential Cybersecurity Controls (ECC) apply to all government organizations in Saudi Arabia, including ministries, authorities, and other public entities, as well as private sector organizations that own, operate, or host Critical National Infrastructures (CNIs). The NCA also encourages other organizations across the Kingdom to adopt these controls as best practices to enhance their cybersecurity.

The ECC is designed to address the cybersecurity needs of all sectors in Saudi Arabia. Every organization must comply with the relevant controls outlined in the document. The specific applicability of each control depends on the organization's business operations and technologies in use. For example:

- **Cloud Computing Controls:**
  Applicable to organizations currently using or planning to use cloud services (Subdomain 4-2).
- **Industrial Control Systems Controls:**
  Required for organizations using or planning to use industrial control systems (Main Domain 5).

This ensures that cybersecurity controls are tailored to each organization's needs and technology landscape.

Empowering Organizations with HCL BigFix: A Comprehensive Cybersecurity Solution

HCL BigFix offers a robust platform tailored to the diverse needs of organizations aiming for NCA compliance. Key USPs of BigFix include:

- **Unified Endpoint and Server Management:**

  BigFix delivers a single platform for managing and securing all endpoints and servers across over 100 operating systems and environments, simplifying endpoint compliance and reducing complexity.

- **Automation of Compliance Enforcement:**

  BigFix automates the enforcement of security policies, ensuring continuous compliance with NCA standards without requiring constant manual intervention.

- **Scalability for Large and Distributed Environments:**

  Built to scale, BigFix is ideal for organizations of all sizes, from small enterprises to large, geographically dispersed entities.

- **Real-Time Monitoring and Reporting:**

  BigFix's real-time monitoring and automated reporting capabilities ensure organizations remain compliant and prepared for audits at all times.

- **Automated Patch Management:**

  BigFix automates patch management across all endpoints and servers, ensuring timely updates and continuous compliance with NCA requirements, significantly reducing the risk of vulnerabilities.

- **CyberFOCUS and IVR:**

  BigFix leverages threat feeds and vulnerability information to help prioritize which vulnerabilities should be addressed first, ensuring the greatest impact on security. It accelerates remediation through out-of-the-box content and powerful automation, making security management more efficient.

Unifying Security Efforts: How BigFix Aligns with NCA's Requirements

Cybersecurity Governance

1-3	Cybersecurity Policies and Procedures	
Objective	To ensure that cybersecurity requirements are documented, communicated and complied with by the organization as per related laws and regulations, and organizational requirements.	
Control Reference Number	Control Clause	BigFix Response
1-3-2	The cybersecurity function must ensure that the cybersecurity policies and procedures are implemented.	**Automate and Enforce Cybersecurity Policies with BigFix** BigFix allows you to configure actions as policies, ensuring they are automatically applied to endpoints based on specific conditions or scheduled timelines. This powerful capability enables seamless implementation and enforcement of cybersecurity policies and procedures throughout the organization, maintaining consistent protection across all endpoints.
1-4	**Cybersecurity Roles and Responsibilities**	
Objective	To ensure that roles and responsibilities are defined for all parties participating in implementing the cybersecurity controls within the organization.	
Control Reference Number	Control Clause	BigFix Response
1-4-1	Cybersecurity organizational structure and related roles and responsibilities must be defined, documented, approved, supported and assigned by the Authorizing Official while ensuring that this does not result in a conflict of interest.	**Role-Based Access Control** BigFix Console roles with role-based access control provide a powerful tool to organize and grant complex permissions within the organization's cybersecurity structure. Custom roles can be defined to establish precise permission sets, which can then be shared among different operators. These roles and permissions can be assigned to console operators, client computers, LDAP groups, and Fixlet sites, ensuring clear documentation, management, and enforcement of roles and responsibilities—effectively preventing conflicts of interest and enhancing organizational security control.
1-4-2	The cybersecurity roles and responsibilities must be reviewed periodically according to planned intervals or upon changes to related laws and regulations.	**Periodic Role Review** The BigFix Deployment Health Checks Dashboard delivers essential insights into inactive operators who haven't logged in for extended periods. This feature helps identify orphaned accounts or those linked to former employees, reinforcing security and ensuring proper account management. Regularly reviewing this data supports effective reassessment of cybersecurity roles and responsibilities, especially in alignment with scheduled evaluations or evolving regulatory requirements.

1-5	Cybersecurity Risk Management	
Objective	To ensure managing cybersecurity risks in a methodological approach in order to protect the organization's information and technology assets as per organizational policies and procedures, and related laws and regulations.	
Control Reference Number	Control Clause	BigFix Response
1-5-3	The cybersecurity risk assessment procedures must be implemented at least in the following cases: 1 Early stages of technology projects. 2 Before making major changes to the technology infrastructure. 3 During the planning phase of obtaining third-party services. 4 During the planning phase and before going live for new technology services and products.	**Risk Assessment through CyberFOCUS** BigFix's Insights for Vulnerability Remediation (IVR), combined with CyberFOCUS (which leverages MITRE APTs and CISA KEV data), and Patch, Vulnerability, and Configuration Compliance analytics dashboards, provides a holistic view of cyber risk in any environment where BigFix agents are deployed. These tools continuously monitor devices and deliver detailed reports that support cybersecurity risk assessments. This capability ensures proactive vulnerability management during the early stages of technology projects, infrastructure changes, third-party service planning, and the launch of new technology services ensuring endpoint compliance.
1-6	Cybersecurity in Information and Technology Project Management	
Objective	To ensure that cybersecurity requirements are included in project management methodology and procedures in order to protect the confidentiality, integrity and availability of information and technology assets as per organization policies and procedures, and related laws and regulations.	
Control Reference Number	Control Clause	BigFix Response
1-6-2	The cybersecurity requirements in project and assets (information/ technology) change management must include at least the following: 1 Vulnerability assessment and remediation. 2 Conducting a configurations' review, secure configuration and hardening and patching before changes or going live for technology projects.	**Vulnerability Assessment and Remediation** BigFix Insights for Vulnerability Remediation (IVR), along with CyberFOCUS and Patch, Vulnerability, and Compliance dashboards, provide in-depth visibility into cyber risks within any environment where the BigFix client agent is deployed. These tools continuously evaluate vulnerabilities and generate detailed reports, ensuring comprehensive oversight for effective vulnerability assessments and remediation. These reports are then integrated into the respective dashboards, providing continuous visibility and enabling proactive management of cyber threats. **Secure Configuration Review and Automated Patching** The vulnerability reports' integration with respective dashboards aligns seamlessly with the cybersecurity requirements for project and asset change management, specifically in conducting vulnerability assessments, remediation, secure configuration reviews, and patching before changes or go-live phases for technology projects.

1-7	Compliance with Cybersecurity Standards, Laws and Regulations	
Objective	To ensure that the organization's cybersecurity program is in compliance with related laws and regulations.	
Control Reference Number	Control Clause	BigFix Response
1-7-1	The organization must comply with related national cybersecurity laws and regulations.	**Compliance and Policy Enforcement** The BigFix Compliance module helps organizations adhere to national cybersecurity laws and internationally-approved agreements. With customizable configuration checklists, patch policies, and automation capabilities, BigFix can ensure that compliance with both national regulations and international commitments is seamless and continuously enforced across the organization's infrastructure.
1-7-2	The organization must comply with any nationally-approved international agreements and commitments related to cybersecurity.	
1-8	Periodical Cybersecurity Review and Audit	
Objective	To ensure that cybersecurity controls are implemented and in compliance with organizational policies and procedures, as well as related national and international laws, regulations and agreements.	
Control Reference Number	Control Clause	BigFix Response
1-8-1	Cybersecurity reviews must be conducted periodically by the cybersecurity function in the organization to assess the compliance with the cybersecurity controls in the organization.	**Ongoing Cybersecurity Compliance Reviews** BigFix offers continuous monitoring through its Insights for Vulnerability Remediation (IVR), CyberFOCUS (integrating MITRE APTs and CISA KEV), and the Patch, Vulnerability, and Configuration Compliance dashboards, across any environment where the BigFix client agent is deployed. These tools provide a real-time evaluation of cybersecurity risks, ensuring organizations consistently comply with cybersecurity controls during periodic reviews.
1-8-2	Cybersecurity audits and reviews must be conducted by independent parties outside the cybersecurity function (e.g., Internal Audit function) to assess the compliance with the cybersecurity controls in the organization. Audits and reviews must be conducted independently, while ensuring that this does not result in a conflict of interest, as per the Generally Accepted Auditing Standards (GAAS), and related laws and regulations.	**Facilitating Independent Audits** BigFix's Role-Based Access Control allows the creation of specialized auditor roles with access to various compliance dashboards, reports, and action histories. This ensures that independent audits and reviews, in line with Generally Accepted Auditing Standards (GAAS) and relevant regulations, can be conducted without conflicts of interest, providing unbiased assessments of the organization's cybersecurity compliance.

Cybersecurity Defense

2-1	Asset Management	
Objective	To ensure that the organization has an accurate and detailed inventory of information and technology assets in order to support the organization's cybersecurity and operational requirements to maintain the confidentiality, integrity and availability of information and technology assets.	
Control Reference Number	Control Clause	BigFix Response
2-1-5	Information and technology assets must be classified, labeled and handled as per related law and regulatory requirements.	**Asset Discovery and Inventory Management** BigFix Asset Discovery and BigFix Inventory enables the discovery and management of hardware and software assets across your IT infrastructure, ensuring they are classified and managed in compliance with relevant laws and regulatory requirements. BigFix Inventory supports software inventory management, monitors license consumption, ensures basic license compliance, and creates a complete hardware inventory, helping your organization meet legal and regulatory standards efficiently.

2-2	Identity and Access Management	
Objective	To ensure the secure and restricted logical access to information and technology assets in order to prevent unauthorized access and allow only authorized access for users which are necessary to accomplish assigned tasks.	
Control Reference Number	Control Clause	BigFix Response
2-2-3	The cybersecurity requirements for identity and access management must include at least the following: 1 User authentication based on username and password. 2 Multi-factor authentication for remote access. 3 User authorization based on identity and access control principles: Need-to-Know and Need-to-Use, Least Privilege and Segregation of Duties. 4 Periodic review of users' identities and access rights.	**Access Management Auditing:** BigFix checklists offer many ways to protect identity and access management including enforcement of strong password policies from CIS and DISA with LDAP integration. These checks can be customized, fine tuned, made into a policy, and enforced on endpoints to ensure continuous compliance. Within the platform, the access to BigFix is controlled by local security and password policies as well to go along with support of SAML 2.0 for MFA.

2-3	Information System and Information Processing Facilities Protection	
Objective	To ensure the protection of information systems and information processing facilities (including workstations and infrastructures) against cyber risks.	
Control Reference Number	Control Clause	BigFix Response
2-3-3	The cybersecurity requirements for protecting information systems and information processing facilities must include at least the following: 1 Advanced, up-to-date and secure management of malware and virus protection on servers and workstations. 2 Restricted use and secure handling of external storage media. 3 Patch management for information systems, software and devices. 4 Centralized clock synchronization with an accurate and trusted source (e.g., Saudi Standards, Metrology and Quality Organization (SASO)).	**Device Hardening** BigFix Enterprise and Workspace UEM solutions deliver comprehensive cybersecurity capabilities, including customized configuration along with advanced malware and virus protection with enforced updates across all endpoints. These solutions also provide features to restrict and secure handling of external storage media. BigFix also provides robust **Patch Management** for various operating systems, middleware, and third-party applications. By maintaining up-to-date protection, BigFix ensures that information systems and processing facilities can meet stringent cybersecurity requirements and stay secure.
2-4	Email Protection	
Objective	To ensure the protection of the organization's email service from cyber risks.	
Control Reference Number	Control Clause	BigFix Response
2-4-3	Secure management and protection against Advanced Persistent Threats (APT), which normally utilize zero-day viruses and malware.	**Protection Against Advanced Persistent Threats (APT)** BigFix leverages the MITRE APT Groups web report, powered by data from the MITRE ATT&CK® Framework, to provide a strategic view of the security posture. This report correlates the tactics, techniques, and procedures used by APTs with BigFix Patch content and the related CVES to identify vulnerabilities present in your environment. The resulting report enables you to quickly prioritize vulnerabilities and take action, empowering you to effectively secure your systems against APTs, including those exploiting zero-day vulnerabilities.

2-5	Networks Security Management	
Objective	To ensure the protection of an organization's network from cyber risks.	
Control Reference Number	Control Clause	BigFix Response
2-5-3	1 Management and restrictions on network services, protocols and ports. 2 Secure management and protection of Internet browsing channel against Advanced Persistent Threats (APT), which normally utilize zero-day viruses and malware.	**Network and Browsing Security Management** BigFix offers powerful capabilities to manage and restrict network services, protocols, and ports at the operating system level using custom fixlets. In addition, BigFix's Compliance Configuration Checklists provide out-of-the-box solutions to measure and enforce compliance for internet browsing applications. This ensures secure management and protection against Advanced Persistent Threats (APT), including zero-day vulnerabilities, by continuously monitoring and securing browsing channels.
2-6	Mobile Devices Security	
Objective	To ensure the protection of mobile devices (including laptops, smartphones, tablets) from cyber risks and to ensure the secure handling of the organization's information (including sensitive information) while utilizing Bring Your Own Device (BYOD) policy.	
Control Reference Number	Control Clause	BigFix Response
2-6-2	The cybersecurity requirements for mobile devices security and BYOD must be implemented.	**Mobile Device and BYOD Security** BigFix Modern Client Management (MCM)/Mobile enables organizations to meet comprehensive cybersecurity requirements for mobile devices and BYOD. It provides full visibility and control over Windows, macOS, iOS, iPadOS, and Android devices, even without a BigFix agent. IT administrators can secure, manage, and monitor both corporate and employee-owned devices, ensuring that updates, compliance, and security policies are enforced. The solution also supports remote wipe, lock, and reboot functions, delivering robust protection and policy enforcement across all mobile devices.
2-6-3	1 Separation and encryption of organization's data and information stored on mobile devices and BYODs. 2 Controlled and restricted use based on job requirements. 3 Secure wiping of organization's data and information stored on mobile devices and BYOD in cases of device loss, theft or after termination/separation from the organization.	**Mobile Device and BYOD Security** BigFix Modern Client Management (MCM)/Mobile enables organizations to meet comprehensive cybersecurity requirements for mobile devices and BYOD. It provides full visibility and control over Windows, macOS, iOS, iPadOS, and Android devices, even without a BigFix agent. IT administrators can secure, manage, and monitor both corporate and employee-owned devices, ensuring that updates, compliance, and security policies are enforced. The solution also supports remote wipe, lock, and reboot functions, delivering robust protection and policy enforcement across all mobile devices.

2-9	Backup and Recovery Management	
Objective	To ensure the protection of organization's data and information including information systems and software configurations from cyber risks as per organizational policies and procedures, and related laws and regulations.	
Control Reference Number	Control Clause	BigFix Response
2-9-3	Ability to perform quick recovery of data and systems after cybersecurity incidents.	**Rapid Recovery and Business Continuity** BigFix ensures high availability and quick recovery of data and systems through its Disaster Server Architecture (DSA) or integration with existing BC/DR tools and plans. By provisioning additional root servers, BigFix enables organizations to recover rapidly from cybersecurity incidents, ensuring maximum service availability and maintaining business continuity, even during disruptions. In addition, using a combination of BigFix's rapid OS and Application deployment tools, it is possible to deploy lost devices or provision new ones from a saved image quickly and recover sooner.

2-10	Vulnerabilities Management	
Objective	To ensure timely detection and effective remediation of technical vulnerabilities to prevent or minimize the probability of exploiting these vulnerabilities to launch cyber attacks against the organization.	
Control Reference Number	Control Clause	BigFix Response
2-10-3	1 Periodic vulnerabilities assessments. 2 Vulnerabilities classification based on criticality level. 3 Vulnerabilities remediation based on classification. and associated risk levels. 4 Security patch management. 5 Subscription with authorized and trusted cybersecurity resources for up-to-date information and notifications on technical vulnerabilities.	**Comprehensive Vulnerability and Remediation Management** BigFix Insights for Vulnerability Remediation (IVR) and CyberFOCUS Security Analytics provide a comprehensive solution for managing and remediating vulnerabilities. BigFix IVR integrates with leading vulnerability scanners like Tenable, Qualys, and Rapid7, allowing for rapid identification and remediation of exploitable vulnerabilities, significantly reducing the time from discovery to remediation. CyberFOCUS helps prioritize vulnerabilities, prescribes effective remediation strategies, and provides real-time insights into improved security outcomes. Alongside automated **Patch Management**, BigFix ensures continuous protection by subscribing to trusted cybersecurity resources, keeping organizations updated on emerging threats.

2-12	Cybersecurity Event Logs and Monitoring Management	
Objective	To ensure timely collection, analysis and monitoring of cybersecurity events for early detection of potential cyber-attacks in order to prevent or minimize the negative impacts on the organization's operations.	
Control Reference Number	Control Clause	BigFix Response
2-12-3	1 Activation of cybersecurity event logs on critical information assets. 2 Activation of cybersecurity event logs on remote access and privileged user accounts. 3 Identification of required technologies (e.g., SIEM) for cybersecurity event logs collection. 4 Continuous monitoring of cybersecurity events. 5 Retention period for cybersecurity event logs (must be 12 months minimum).	**Comprehensive Event Logging** BigFix provides detailed logging across all systems, from basic informational logs to advanced debugging, ensuring thorough tracking of cybersecurity events. With seamless integration into SIEM solutions like Splunk, BigFix enables efficient collection and consolidation of event logs, supporting continuous monitoring and compliance with logging requirements.

2-15	Web Application Security	
Objective	To ensure the protection of external web applications against cyber risks.	
Control Reference Number	Control Clause	BigFix Response
2-15-3	1 Use of web application firewall. 2 Adoption of the multi-tier architecture principle. 3 Use of secure protocols (e.g., HTTPS). 4 Clarification of the secure usage policy for users. 5 Multi-factor authentication for users' access.	**Secure Web Application Management** BigFix leverages a multi-tier architecture, supporting both local and remote databases, with a robust WebUI accessible via any supported browser. The WebUI ensures security through HTTPS protocols and integrates SAML 2.0 for multi-factor authentication. This approach aligns with secure architecture principles, protects user access, and enhances the overall security of web applications in compliance with modern cybersecurity standards.

Industrial Control Systems Cybersecurity

5-1	Industrial Control Systems (ICS) Protection	
Objective	To ensure the appropriate and effective cybersecurity management of Industrial Controls Systems and Operational Technology (ICS/OT) to protect the confidentiality, integrity and availability of the organization's assets against cyber attacks (e.g., unauthorized access, destruction, spying and fraud) in line with the organization's cybersecurity strategy and related and applicable local and international laws and regulations.	
Control Reference Number	Control Clause	BigFix Response
5-1-3	1 Strict limitation on the use of external storage media. 2 Periodic review and secure configuration and hardening of industrial, automated, support systems, and devices. 3 Vulnerability management for industrial control systems and operational technology (ICS/OT). 4 Patch management for industrial control systems and operational technology (ICS/OT).	**Simplified Compliance and Cybersecurity with BigFix** BigFix Compliance provides customizable tools like configuration and hardening checklists, patch policies, and automation to help meet regulatory requirements. It also includes checks to ensure the secure handling of external storage media. Additionally, with BigFix CyberFOCUS Security Analytics, critical vulnerabilities are identified, prioritized, and fixed in near real-time, improving collaboration between IT and security teams. BigFix IVR also works with vulnerability scanners to quickly identify and remediate security risks on any ICS/OT devices where the BigFix agent is installed. BigFix has **patch management** support for over 100 different OSs and many applications and middleware, along with the ability to build custom patch content to keep devices up to date.