Prepared 21 May 2025

How AgendaWorx Assists Boards in Complying with the FSCA's New Cybersecurity Standard

Effective 1 June 2025, the Financial Sector Conduct Authority (FSCA) in South Africa will implement a new cybersecurity standard aimed at enhancing the protection of sensitive financial data and ensuring robust governance in the financial sector. For boards of financial institutions, compliance with this standard is critical to safeguard board-related processes and documents. AgendaWorx, as a secure online board portal, offers a comprehensive solution to help boards meet these requirements through its advanced security protocols and streamlined document management. This report explores how AgendaWorx aligns with the FSCA's cybersecurity standard and ensures compliance for board operations.

Overview of the FSCA Cybersecurity Standard

The FSCA's cybersecurity standard, effective 1 June 2025, mandates financial institutions to implement stringent measures to protect data, ensure system integrity, and mitigate cyber risks. While the exact requirements may vary, typical cybersecurity standards for financial institutions include:

1. **Data Encryption**: All sensitive data, both at rest and in transit, must be encrypted using industry-standard protocols.
2. **Access Controls**: Robust user authentication and authorisation mechanisms, including multi-factor authentication (MFA), to prevent unauthorised access.
3. **Regular Security Assessments**: Periodic vulnerability scans, penetration testing, and security audits to identify and address risks.
4. **Incident Response and Recovery**: Defined recovery time objectives (RTO) and recovery point objectives (RPO), along with disaster recovery and backup processes.
5. **Compliance with International Standards**: Adherence to frameworks like ISO 27001 for information security management.
6. **Secure Infrastructure**: Use of secure cloud environments and perimeter security controls, such as firewalls.

7. **Data Integrity and Confidentiality**: Ensuring no sensitive information is transmitted via unsecured channels, such as email.

AgendaWorx's security protocols are designed to meet or exceed these requirements, providing boards with a secure, compliant platform for managing sensitive documents and processes.

How AgendaWorx Ensures Compliance

AgendaWorx offers a secure board portal that eliminates the need for emailing sensitive documents, ensuring all board-related activities occur behind its robust firewall. Service providers, ***such as company secretaries or auditors, can upload any documents directly to AgendaWorx***, allowing board members to access them securely and efficiently. Below is a detailed breakdown of how AgendaWorx addresses the FSCA's cybersecurity standard requirements:

1. **Data Encryption**
    - **AgendaWorx Feature**: All documents and data, including audio recordings, are encrypted using AES-256CBC, a 256-bit encryption standard recognised as industry-leading. Documents are unencrypted only for viewing and re-encrypted upon upload.
    - **FSCA Compliance**: This ensures that sensitive board documents, such as meeting agendas, financial reports, and resolutions, are protected at rest and in transit, meeting the FSCA's encryption requirements.
2. **Access Controls**
    - **AgendaWorx Feature**: User authentication requires a username and a complex password (minimum 14 characters, including uppercase, lowercase, digits, and no consecutive numbers). Multi-factor authentication (MFA) is mandatory for initial device logins and when using new browsers or devices. Administrators can enforce password changes if risks are detected.
    - **FSCA Compliance**: These measures prevent unauthorised access to board portals, aligning with the FSCA's requirements for robust authentication and access control.
3. **Regular Security Assessments**
    - **AgendaWorx Feature**: Annual penetration testing is conducted by a CREST-certified third-party firm, adhering to international standards (PTES, OWASP, OSSTMM, NIST). The latest test in November 2024 confirmed zero medium-to-high vulnerabilities. Monthly vulnerability scans by an external

server specialist and quarterly in-house assessments further ensure system integrity.

- **FSCA Compliance**: Regular testing and scanning meet the FSCA's mandate for proactive identification and mitigation of cyber risks.

4. **Incident Response and Recovery**
    - **AgendaWorx Feature**: Defined RTO and RPO are part of the contracting process, with incident reports maintained for all support cases. Daily backups are managed by AWS Backup, stored on Amazon S3 for seven days, with the main server in Ireland and backups in Germany to reduce geopolitical risks. Data and backups are encrypted at source and in transit.
    - **FSCA Compliance**: These disaster recovery and backup processes ensure minimal data loss and rapid recovery, aligning with the FSCA's incident response requirements.
5. **Compliance with International Standards**
    - **AgendaWorx Feature**: AgendaWorx is ISO 27001 certified, demonstrating adherence to global information security management standards.
    - **FSCA Compliance**: ISO 27001 certification provides assurance that AgendaWorx's security practices meet international benchmarks, supporting FSCA compliance.
6. **Secure Infrastructure**
    - **AgendaWorx Feature**: Hosted on the AWS Global Cloud Infrastructure, AgendaWorx benefits from AWS's secure, reliable environment. Perimeter security includes a Web Application Firewall (With Secure) and 24/7 for around-the-clock security and threat scans. Security Groups is utilised to limit access. AWS's shared responsibility model ensures that infrastructure-level security is managed by AWS, while AgendaWorx handles application-level security.
    - **FSCA Compliance**: The use of a secure cloud environment and perimeter controls meets the FSCA's requirements for protected infrastructure.
7. **Data Integrity and Confidentiality**
    - **AgendaWorx Feature**: Unlike traditional methods that rely on email, AgendaWorx ensures all board documents and communications remain within its secure portal. Service providers upload documents directly, eliminating the risk of interception or unauthorised access via email.

    - **FSCA Compliance**: By keeping all activities behind its firewall, AgendaWorx ensures the confidentiality and integrity of sensitive board information, addressing the FSCA's emphasis on secure data handling.

Additional Security Measures for FSCA Compliance

To further align with the FSCA's cybersecurity standard and address additional board cyber risks, AgendaWorx supports the following measures, which can be implemented by boards or enforced through AgendaWorx configurations:

- **Device Security**:
    - **Automatic Laptop Locking**: Boards can enforce policies to lock laptops after five minutes of inactivity, complementing AgendaWorx's secure access controls. While AgendaWorx itself is a cloud-based portal, this policy ensures devices accessing the portal are protected.
    - **Anti-Malware Protection**: Boards should mandate approved anti-malware software with regular updates on all devices accessing AgendaWorx, ensuring no malware compromises portal access.
    - **Mobile Device Security**: AgendaWorx supports secure access from mobile devices, and boards can implement mobile device management (MDM) solutions to enforce security settings, such as encryption and remote wipe capabilities, on devices used by board members.
- **Training and Awareness**:
    - **Phishing Training**: AgendaWorx recommends boards conduct monthly phishing training to protect members from social engineering attacks that could compromise login credentials.
    - **Security Awareness Training**: Regular security awareness sessions for board members and staff should be facilitated to reinforce best practices, such as recognising suspicious links or securing devices, enhancing the overall security posture when using AgendaWorx.
- **AI Usage**:
    - **Secure AI Integration**: To prevent data leaks from using external AI tools like ChatGPT or Grok, AgendaWorx integrates secure AI functionalities via APIs within the portal, ensuring sensitive board data remains protected.
- **File Access Restrictions**:
    - **Restricting Downloads**: AgendaWorx can be configured to restrict file downloads, allowing board members to view documents only within the

secure portal environment. This minimises the risk of sensitive files being stored on unsecured devices.

- **Password Policies**:
    - **Strong, Unique Passwords**: In addition to complex password requirements, AgendaWorx encourages policies for non-reused passwords and regular password updates to further reduce the risk of credential compromise.
- **Software Updates**:
    - **Regular Updates**: AgendaWorx's monthly vulnerability scans and patching are complemented by recommending that boards establish schedules for regular software updates on devices accessing the portal, ensuring all systems remain secure.
- **Vendor Vetting**:
    - **Third-Party Security**: AgendaWorx's own security is rigorously vetted (e.g., CREST-certified penetration testing), and boards are advised to implement vendor risk assessments for other third-party providers to ensure their security practices align with FSCA standards.
- **Logging and Monitoring**:
    - **Access Tracking**: AgendaWorx supports logging and monitoring solutions to track access to sensitive data and use 24/7 to detect suspicious activity on the server, providing boards with visibility into portal usage and potential threats.
- **Cyber Insurance Scope**:
    - **Comprehensive Coverage**: AgendaWorx's R10,000,000 cyber insurance through Hollard (ITOO) provides protection, but boards should ensure their own cyber or trustee insurance policies cover incidents arising from negligent password practices or data leaks via unprotected devices.

Additional Benefits for Boards

Beyond compliance, AgendaWorx enhances board efficiency and security through:

- **Centralised Document Management**: Board packs, minutes, and resolutions are stored securely in one place, accessible only to authorised users.
- **Global Accessibility**: Board members can access documents securely from any device, with MFA ensuring protection across browsers and devices.

- **Audit Readiness**: Detailed security reports (penetration tests, vulnerability scans) are available on request, simplifying compliance audits.

Conclusion

AgendaWorx is uniquely positioned to help boards comply with the FSCA's cybersecurity standard effective 1 June 2025. Its robust encryption, stringent access controls, regular security assessments, secure cloud infrastructure, and additional features like restricted downloads, secure AI integration, and support for device security policies address all key requirements of the standard. By eliminating email-based document sharing, enabling direct uploads within its secure portal, and supporting comprehensive security measures, AgendaWorx ensures that board-related processes remain confidential, efficient, and compliant. For financial institutions seeking a trusted partner to navigate the evolving cybersecurity landscape, AgendaWorx offers a proven, secure solution.