Consolidated Compliance Report: EcoCash

1. Zimbabwe Data Protection Act (ZDPA) Compliance

EcoCash has made significant progress in aligning its operations with the Zimbabwe Data Protection Act (ZDPA). The ZDPA mandates that companies collect, store, and process personal data responsibly, ensuring data security and privacy for users. In compliance with the ZDPA, EcoCash has implemented the following measures:

1.1 Data Collection and Processing:

- Personal data is collected only with user consent and for specific, legitimate purposes.
- Users are informed about the purpose of data collection and their rights under the ZDPA.

1.2 Data Security Measures:

- EcoCash employs encryption technologies to protect personal data both in transit and at rest.
- Secure data access controls are implemented, limiting access to authorized personnel only.

1.3 User Rights and Access:

- Users have the right to request access to their personal data, rectify inaccuracies, and request data deletion.
- Procedures are in place to promptly respond to user requests within the statutory timeframes.

1.4 Data Breach Management:

- EcoCash has implemented a robust data breach response plan to detect and mitigate potential breaches.
- Users are notified promptly in case of a data breach affecting their personal information.

In conclusion, EcoCash has made considerable strides in achieving compliance with the ZDPA, with continuous improvements being made to its data protection framework.

2. PCI DSS Compliance

EcoCash has undertaken comprehensive measures to comply with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is a set of security standards designed to protect card payment data. Below is an overview of EcoCash's PCI DSS compliance progress:

2.1 Secure Network and Systems:

- EcoCash uses firewalls, intrusion detection/prevention systems, and other security technologies to protect cardholder data from unauthorized access.
- All systems processing payment card information are isolated from other networks to minimize exposure to potential threats.

2.2 Data Encryption and Protection:

- Cardholder data is encrypted both during transmission and while stored.

- Sensitive payment data, such as full card numbers and CVV, are never stored on systems unless absolutely necessary, and such data is encrypted using strong encryption standards.

2.3 Access Control:

- Access to payment card data is restricted based on a ‘need-to-know’ basis, ensuring that only authorized personnel have access.
- Robust user authentication methods, including multi-factor authentication, are employed for personnel accessing payment card data.

2.4 Regular Testing and Monitoring:

- EcoCash conducts regular vulnerability assessments and penetration testing to identify and mitigate security weaknesses.
- Continuous monitoring systems are in place to detect and respond to any unauthorized access or suspicious activity in real time.

In conclusion, EcoCash is progressing well with its PCI DSS compliance, with most requirements fully implemented and regular audits to ensure adherence to the standards.

3. ISO 27001 Audit Compliance

EcoCash has undertaken an ISO 27001 audit to ensure that its Information Security Management System (ISMS) meets international standards for security. ISO 27001 is a globally recognized standard for managing risks related to information security. Below is a summary of EcoCash's ISO 27001 compliance progress:

3.1 Information Security Policies:

- EcoCash has developed comprehensive information security policies, ensuring that security measures are aligned with organizational goals and industry standards.
- The policies are regularly reviewed and updated to reflect changes in the business environment and emerging security threats.

3.2 Risk Assessment and Management:

- EcoCash conducts regular risk assessments to identify and evaluate potential risks to the confidentiality, integrity, and availability of information.
- A risk treatment plan has been established, detailing actions to mitigate, transfer, or accept risks based on their potential impact.

3.3 Internal Audits and Reviews:

- Regular internal audits are conducted to assess the effectiveness of the ISMS and identify areas for improvement.
- Audits focus on ensuring that security controls are operating as intended and that corrective actions are taken to address any deficiencies.

3.4 Staff Awareness and Training:

- EcoCash has implemented an ongoing staff awareness program to ensure that all employees are trained on information security best practices.
- This includes training on topics such as data handling, phishing prevention, and responding to security incidents.

3.5 Incident Management and Continuous Improvement:

- A formal incident management process is in place to detect, respond to, and recover from information security incidents.

- EcoCash continuously monitors its information security environment, implementing improvements based on audit findings and security incidents.

In conclusion, EcoCash has made significant progress in achieving ISO 27001 compliance, with its ISMS effectively managing information security risks and aligning with international best practices.

4. Gaps and Key Issues

Despite significant progress in all three compliance areas, several gaps and key issues have been identified that require attention:

1. Data Breach Management (ZDPA): Although EcoCash has a breach response plan, there is a need for more comprehensive testing of the plan under various real-world scenarios to ensure it operates effectively during an actual data breach event.
2. Payment Card Data Storage (PCI DSS): While EcoCash has strong encryption standards in place, there is a need to continually assess whether the minimum necessary data is stored to reduce potential risk and comply with PCI DSS requirements.
3. Risk Treatment Plans (ISO 27001): Although EcoCash conducts regular risk assessments, a more structured and continuous evaluation of risk treatment plans would ensure that newly emerging risks are addressed in a timely manner.
4. Staff Training and Awareness (ISO 27001 and PCI DSS): There is a need for ongoing updates to staff training programs to address emerging threats such as new forms of social engineering and cyber-attacks that may not have been included in previous sessions.

In summary, while EcoCash is making commendable progress in meeting compliance standards, addressing these gaps will further strengthen its security posture and ensure long-term resilience against data-related threats.