VALUEFY INTERNAL CYBER SECURITY AUDIT REPORT

Cyber Security Internal Audit Report Prepared for Valuefy Technologies Private Limited

Table of Contents

1.0 Executive Summary

The objective of the audit was to assess the overall cybersecurity posture of Valuefy and also with respect to its Wealthfy EAM Application.The intended goal is to assess the effectiveness of security policies and the respective security controls in place.The cybersecurity audit also includes evaluating GDPR Compliance for the Wealthfy EAM Application.The purpose of the audit was to assist the V aluefy executive team in developing a strategy for managing cyber security.

A summary of the recommendations made during the cyber security audit is detailed in Section 2. The recommendations can be categorised as Non-Technical (NT), Technical (T) and Physical (P)

2.0 Cyber Assessment Findings & Recommendations

2.1 Risk Management

During the course of the audit it has been observed that risk management processes are found lacking in the Wealthfy EAM Application.It would mean that any changes in the application that are executed are not evaluated for any risks that may get introduced as a part of a new change or any implementation.

Recommendations

- Establish a robust risk management process in context to the security of the Wealthfy EAM Application. (NT)
- Conduct a risk assessment at regular intervals of the organisations assets and apply security controls wherever applicable (NT)

2.2 Training and Awareness Program

During the course of the audit and while interviewing Valuefy staff members it has been observed that new hires are required to undergo mandatory information security awareness sessions.However training and awareness programs were found to be inadequate as older employees are not required to undergo mandatory training and awareness sessions.It has been observed that GDPR awareness sessions have been conducted for staff members however it was carried out in an adhoc manner and new employees have not undergone GDPR awareness sessions.

Recommendations

- Provide security awareness training to all staff members on regular basis and communicate security updates on regular intervals. (NT)
- GDPR awareness training sessions should be provided to all staff members and checks should be carried at regular intervals to identify the staff members who need to undergo mandatory GDPR training sessions. (NT)

2.3 Policies and Procedures

During the course of the audit Valuefy's information security policy was reviewed along with other relevant policies such as acceptable use policy , DR policy ,antivirus Policy. However from a security standpoint other relevant policies such as Internet Usage policy , remote access policy , data classification policy , risk assessment policy , malware protection policy was found missing.

Recommendations

- Document internet usage policy , data classification policy , remote access policy , risk assessment policy , malware protection policy . (NT)
- Document any other relevant internal processes and procedures and technical work instrusctions that provides extensive coverage of cyber security measures. (NT)

2.4 Incident Reporting & Response

During the course of the audit the incident response of Valuefy was reviewed and was found to be adequate however during interviewing Valuefy staff members it was observed that a lack of awareness persists with regards to incident reporting and response.

Recommendations

- User awareness sessions should be conducted to bring awareness amongst staff members with respect to incident reporting. (NT)

2.5 Business Continuity Management

During the course of the audit Valuefy's BCP policy was reviewed and RTO and RPO values were observed to be of one hour and four hours duration.During the course of interaction with key personnel of Wealthfy's EAM team it was observed that tabletop and structured walkthrough tests have been conducted at Valuefy.However full scale testing or parallel testing exercise is yet to be conducted at Valuefy.The RTO and RPO metrics effectiveness can only be observed in practice only after conducting a full scale test.

Recommendations

- Test the business continuity plan or arrangement by conducting a full scale interruption test. (T)
- Review the RPO and RTO values post conducting a full scale interruption test to see if it meets the intended values. (NT)

2.6 Third Party Inspections

While interviewing key personnel of the Wealthfy's EAM Application team it was observed that Valuefy works with its partners and shares data with the partners.However there are no established provisions in place to validate the security controls put in place by Valuefy channel partner organizations.

Recommendations

- Carry out third party provider risk assessments. (NT)
- Assess and ask for an indepedent audit report of the partner organizations. (NT)

2.7 Third Party Contracts

During the course of the audit it was discovered that Valuefy's EAM Application team works with multiple partner organizations.It has been observed that while Valuefy does have contract agreements with some of the partners and with some partners contracts are missing.As partner organizations are leveraging client data from Valuefy applications it is important to have contract agreements in place with all partners and necessary provisions should be put in place in contract to ensure due diligence is carried out by partner organizations.

Recommendations

- Ensure due diligence is observed by having contracts in place with all partner organizations. (NT)
- Ensure necessary provisions are put in place in contract to ensure partners are compliant with information security requirements related to client data and with respect to GDPR Compliance. (NT)

2.8 Secure Configuration

During the course of the audit evaluation of the configuration was done.Valuefy maintains a standard build and rollout across the environments.Valuefy adopts a standard process for secure configuration across environments.

Recommendations

- Maintain configuration change history for tracking and auditing requirements.

2.9 Security Updates & Patches

During the course of the audit it has been discovered that antivirus software has been installed on allocated laptops to employees however there is not any documented procedure for applying any security updates or patches.

Recommendations

- Document and implement a patching policy for all hardware and

applications. (T)

- Apply security patches and updates at appropriate intervals on allocated system resources. (T)

2.10 Breach Management

During the course of the audit it has been observed that there is not any breach incident and notification policies or procedure defined at Valuefy.Any such data breach incident notification is usually done in an adhoc manner.From the perspective of GDPR it is necessary to have an upto data breach response plan and to maintain a data breach register and both these entities are missing in the existing Valuefy process hierarchy.

Recommendations

- Create a data breach incident and notification policy and procedure. (NT)
- Maintain an upto date data breach response plan. (NT)
- Maintain a data breach register including facts related to the breach, effects and remedial actions taken to resolve the issue. (NT)

2.11 Mobile devices, mobile working and removable media

During the course of the audit it was discovered that there is not BYOD policy for accessing Wealthfy EAM application via the mobile devices.Since the users are accessing the application via mobile devices it is important to have policies that provide assurance that the client data will not be mishandled on mobile Devices.

Recommendations

- Document a BYOD policy for internal and external users. (NT)

2.12 Data Storage

During the course of the audit it was observed that Valuefy's data retention policy was Reviewed and was found to be adequate.Valuefy encrypts all the data at rest and in Transit.In addition to this Valuefy maintains an appropriate data disposal policy.

2.13 Development

During the course of the interaction as a part of the internal audit with key stakeholders of the Wealthfy EAM Application team it was observed that Valuefy has a well established secure code review process and a well designed System engineering and production release process.However lack of detailed documentation with regards to development has been found lacking.

Recommendations

- Document the development process. (NT)
- Maintain detailed documentation related to code (T)

2.14 Security Monitoring

During the course of the audit it was observed that Valuefy has not yet implemented any security monitoring tools for identifying , detecting and preventing any cyber security threats in real time.There is not any IDS / IPS tool installed to detect or prevent threats.Neither is there any SIEM tool provisioned that can be used to collect events and generate alerts.

Recommendations

- Introduce network and device monitoring. (T)
- Introduce an IDS (intrusion detection solution). (T)
- Introduce a SIEM solution in the existing environment (T)

2.15 Data Privacy Impact Assessments (DPIA)

During the course of the audit it was observed that Valuefy has no previous history of carrying out any data privacy impact assessments.As a result there is no established process to identify any data privacy related risks.

Recommendations

- Initiate data privacy impact assessment exercise at regular intervals . (NT)
- Establish a process for detecting changes in privacy risks and review DPIA for changed risks . (NT)

3.0 Conclusion

Valuefy is in the process of developing a robust cyber security strategy to support its future requirements.Twenty-seven (27) recommendations were made following the high-level cyber security audit.The list of recommendations also are inclusive of the ones from a GDPR compliance perspective.The internal audit assessment was carried over a period of four weeks.Based on the discussions with Valuefy management team the implementation of the audit report recommendations will be carried out over a time frame of next twelve to sixteen weeks.