

# Third-Party Assessment

## Date: 23rd November 2023

# Risk Summary

Chameleon Website Teams security has an acceptable level of security maturity. Chameleon Website Teams security has demonstrated commitment to the security of their services.

Strong track record of transparency and maintaining the security of their product/service and their own supply chain.

Overall the risk is low, and the impact of a vendor compromise is low due to the classification & volume of records

Based on the review of responses to the security questionnaire, and the review of provided documentation, there is reasonable assurance the Chameleon Website Teams security has satisfactory information security controls.

## Risk Finding Count

| Risk Rating | Count |
| --- | --- |
| Significant | 0 |
| Major | 0 |
| Moderate | 0 |
| Minor | 3 |

# 

# Introduction:

This report features the security questionnaire sent to the Chameleon website team to complete, for myself to review.

# Tools used:

# Excel

# Word

# 

# Scope of Testing

The scope of the testing included a range of questions revolving around the ISO27001:2013 standards. ISO 27001 is an international standard for information security management systems (ISMS). It provides a systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability. The latest version of ISO 27001 before my last update was ISO/IEC 27001:2013.

# 

# Methodology

A third-party assessment, often referred to as an external or independent assessment, is a process where an external entity evaluates the performance, compliance, or security of another party, typically a business or organisation. This type of assessment can cover various aspects, including information security, compliance with regulations, quality management, or overall business operations. Here is a general methodology for a third-party assessment:

1. **Define Scope and Objectives:**
   * Clearly define the scope of the assessment, outlining what areas or processes will be evaluated.
   * Establish the specific objectives and goals of the assessment, considering the needs and concerns of all involved parties.
2. **Pre-assessment Planning:**
   * Develop a detailed plan that includes the assessment methodology, assessment criteria, and the assessment timeline.
   * Identify the key stakeholders and involve them in the planning process.
   * Determine the resources required for the assessment, including personnel, tools, and documentation.
3. **Information Gathering:**
   * Collect relevant information about the organisation being assessed, such as policies, procedures, documentation, and any historical data.
   * Interview key personnel and stakeholders to gain insights into the organisation's processes and practices.
4. **Assessment Execution:**
   * Conduct on-site or remote assessments based on the predefined methodology.
   * Use a combination of interviews, document reviews, and technical evaluations, depending on the nature of the assessment.
   * Evaluate the organisation against established standards, regulations, or best practices.
5. **Data Analysis:**
   * Analyse the collected data to assess the organisation's performance, compliance, or security posture.
   * Identify strengths, weaknesses, opportunities, and threats.
6. **Report Generation:**
   * Prepare a comprehensive assessment report that includes findings, recommendations, and any identified areas for improvement.
   * Clearly communicate the results to the organisation being assessed and, if applicable, to other stakeholders.
7. **Feedback and Review:**
   * Share the draft assessment report with the organisation for feedback and clarification.
   * Address any concerns or questions raised by the assessed organisation.
   * Finalise the report based on the feedback received.
8. **Presentation and Delivery:**
   * Present the final assessment findings to the relevant stakeholders.
   * Discuss recommendations and potential improvement strategies.
9. **Follow-up and Monitoring:**
   * Provide ongoing support and monitoring if required.
   * Assess the organisation's progress in implementing recommended changes and improvements.
10. **Continuous Improvement:**
    * Gather lessons learned from the assessment process.
    * Use feedback to refine and improve future assessment methodologies.

# Results

The results can be found below, with three findings identified and set for remediation.

## Engagement Scope

**In Scope**

This TPA covers the following:

* General security governance assessment of the Chameleon Website Teams security maturity;
* Focused assessment on the security controls and mechanisms that the vendor has in place, to protect customer and corporate data.

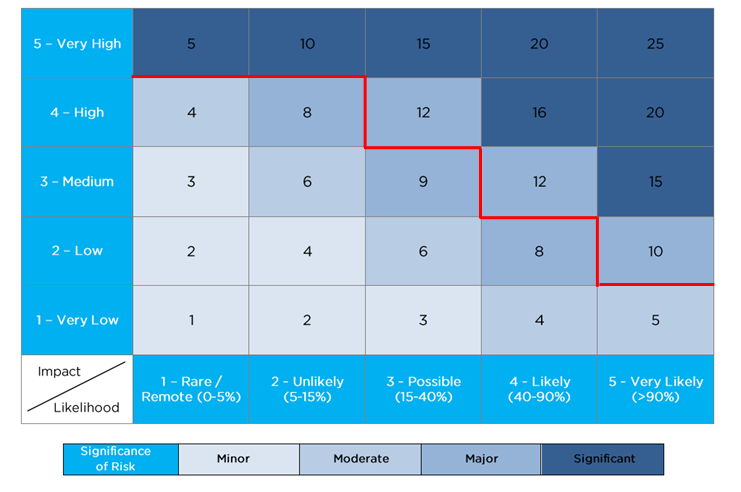
Control Standards Alignment

| **Control Group** | **Control Effectiveness** |
| --- | --- |
| Application Development | Effective |
| Asset Management & Configuration Management | Effective |
| Boundary Defence | Effective |
| Cyber Resilience | Not Effective |
| Data & Information Protection | Not Effective |
| Education and Awareness | Not Effective |
| Endpoint Security & Malware Defences | Effective |
| Identity & Access Management | Effective |
| Incident & Problem Management | Effective |
| IT Change Management | Effective |
| Network & Wireless Security | Effective |
| Platform & Cloud Security | Effective |
| Security Operations & Vulnerability Management | Effective |
| Service Design & Technology Resilience | Effective |
| Physical Security | Effective |
| Third Party Management | Effective |
| Security Governance | Effective |

# Risk Assessment

| Security Domain | | Observation & Recommendation |
| --- | --- | --- |
| Application Development | | No gaps observed |
| Asset Management & Configuration Management | | No gaps observed |
| Cyber Resilience | | Gaps observed  **Issue**  The Chameleon website team has not tested their backups within the last 12 months.  **Recommendation**:  Regularly test and validate backups to ensure their effectiveness in the event of a cyber incident or data loss. Regular testing helps identify any issues with the backup process, such as incomplete or corrupted backups and ensures a timely recovery in case of a security incident. Establish a routine schedule for backup testing, considering the criticality of the data and the frequency of system changes or updates. This practice is essential for maintaining a robust cybersecurity posture and ensuring the ability to recover data in case of a cyberattack or other unforeseen events.  **Issue**:  The Chameleon website team has not conducted a penetration test on the website  **Recommendation**:  Conduct a thorough penetration test on the Chameleon website to identify and address potential vulnerabilities. Penetration testing, also known as ethical hacking, involves simulating real-world cyberattacks to evaluate the security of a system. This proactive approach helps uncover weaknesses in the website's defences, including potential entry points for attackers. Schedule regular penetration tests to be conducted at appropriate intervals or in response to significant changes in the website's infrastructure or code. Address the identified vulnerabilities promptly to enhance the overall security posture of the website and mitigate the risk of exploitation by malicious actors. Regular testing is crucial for staying ahead of evolving cyber threats and ensuring the ongoing protection of sensitive information and user data. |
| Data & Information Protection | | Gaps Observed  **Issue**:  The Chameleon website team have stated that they do not have encryption for any confidential data stored.  **Recommendation**:  Implement encryption measures to protect confidential data stored on the Chameleon website. Encryption is a crucial security mechanism that converts sensitive information into a coded format, making it unreadable to unauthorised individuals. Apply encryption protocols, such as HTTPS for web communication and encryption algorithms for stored data, to safeguard sensitive information from potential breaches. Prioritise the encryption of personally identifiable information (PII), financial data, and other confidential details. Additionally, ensure that encryption protocols are correctly configured and up-to-date to maintain the effectiveness of the security measures. Regularly assess and update encryption practices in alignment with industry standards to mitigate the risk of data breaches and enhance overall cybersecurity. |
| Education and Awareness | | Gaps Observed  **Issue**:  No cyber security awareness training has been conducted within Chameleon.  **Recommendation**:  Initiate comprehensive cybersecurity awareness training programs for all personnel within Chameleon. Cybersecurity awareness is a fundamental component of a robust security posture, and ensuring that employees are well-informed helps prevent and mitigate potential security risks. Develop training modules that cover essential topics such as recognising phishing attempts, password best practices, secure internet usage, and the importance of regular software updates. Schedule regular training sessions and consider incorporating simulated phishing exercises to reinforce the importance of vigilance against cyber threats. Establish a culture of cybersecurity awareness, emphasising the role each employee plays in safeguarding the organisation's information and assets. Continuous training and reinforcement are key to building a resilient workforce against evolving cyber threats. |
| Endpoint Security & Malware Defences | | No gaps observed |
| Identity & Access Management | | No gaps observed |
| Incident & Problem Management | | No gaps observed |
| IT Change Management | | No gaps observed |
| Network & Wireless Security | | No gaps observed |
| Platform & Cloud Security | | No gaps observed |
| Security Operations & Vulnerability Management | | No gaps observed |
| Service Design & Technology Resilience | | No gaps observed |
| Physical Security | | No gaps observed |
| Third Party Management | | No gaps observed |
| Security Governance | | No gaps observed |

## Risk Rating[[1]](#footnote-0)

****

# Key Considerations

Below are the key points discussed while performing the TPA – Some of these were not mentioned in the scoping documents but understood will be incorporated during the delivery/implementation.

* {insert any assumptions or considerations identified during the BO interviews}
* Risks are assessed based on the Risk Management framework.
* All risks identified are based on Residual Risk which is the risk position that remains if the project doesn’t implement the recommended mitigating / compensating controls outlined in this document.

1. [↑](#footnote-ref-0)