WWiSE
WORLD WIDE INDUSTRIAL & SYSTEMS ENGINEERS

ISO 27001:2022 ISMS Internal Audit

July 2025

BASED ON:

STANDARDS

- ISO/IEC 27001:2022 Information Security Management System

FOR

- Owethu Managed Services (Pty) Ltd

MEMBERSHIPS, ACCREDITATIONS, AND PARTNERSHIPS

DOCUMENT HISTORY

Version	Date Released	Comments
1	Wednesday, 09th of July 2025	GAP assessment based on ISO/IEC 27001:2022 Information Security Management System.

CONTENTS

EXECUTIVE SUMMARY

This document presents the findings emanating from the internal audit conducted by Worldwide Industrial & Systems Engineers (Pty) Ltd ("WWISE") on Owethu Managed Services (Pty) Ltd. The Gap assessment was conducted on Wednesday, 09th of July 2025.

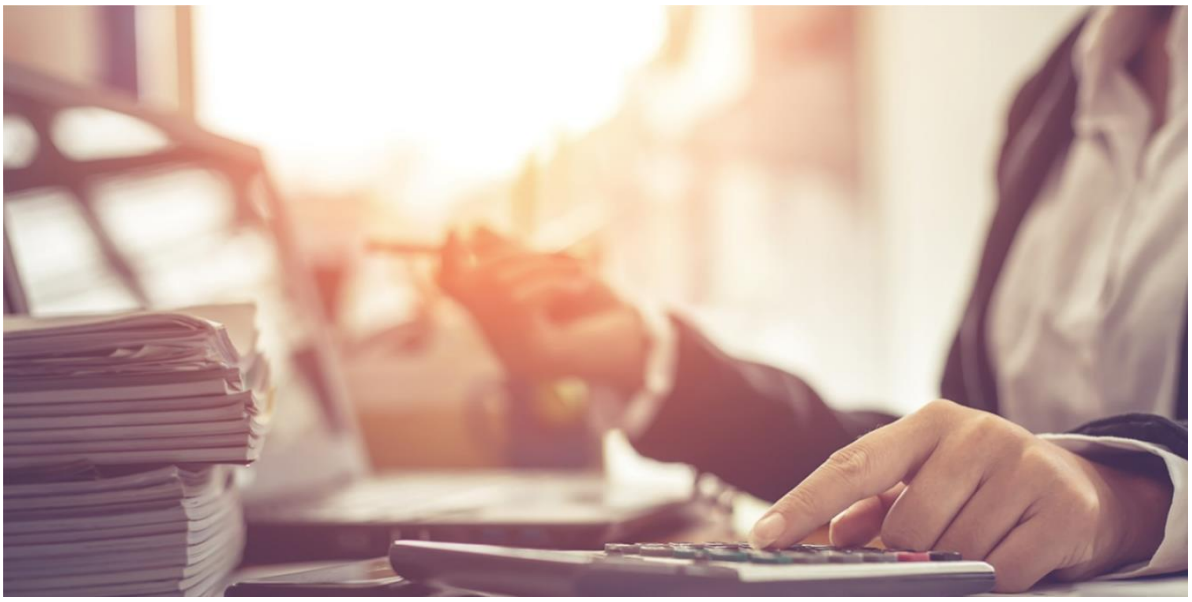
OBJECTIVE

The objective of the gap assessment was to evaluate the adequacy and effectiveness of the measures taken by Owethu Managed Services to meet the performance obligations of the ISO/IEC 27001:2022 Information Security Management System standard.

SCOPE

WWISE has been appointed as the independent internal audit organisation that shall evaluate the compliance and conformance to the above standard, and any other related requirements for Owethu Managed Services. During the internal gap, WWISE assessed Owethu Managed Services systems and the effectiveness of its processes to evaluate compliance across the audit period.

This internal audit report also identifies opportunities for improvement between Owethu Managed Services' current practices and the referenced standard to ensure continuous improvement that is reflective of the requirements of Owethu Managed Services' processes, as well as statutory and regulatory requirements.



APPLICABLE FUNCTIONS

Applicable functions include:

1 Information Security Management System

2 ICT Operations and Governance

3 Human Resources

4 Finance

5 Facilities

6 Sales

NON-APPLICABLE CONTROLS

- N/A

GAP AUDIT REPORT

AUDITEES AND AUDIT TEAM

AUDITEE(S)	Owethu Managed Services (Pty) Ltd
LEAD AUDITOR	Peter Mafatshe
AUDIT TEAM	Peter Mafatshe and Olebogeng Hlabathi

FINDING/ NON-CONFORMITY GRADING

MAJOR GAP

A major gap is a significant failure to meet key requirements or standards, which may directly impact business operations and objectives. It indicates a critical lapse, either in failing to implement or maintain necessary processes.

- Examples: Failure to perform data backups, lack of management reviews, absence of internal audits, or serious issues with training or customer feedback processes.
- Impact: Affects certification status and requires immediate correction, often necessitating additional audits and possibly incurring costs.

MINOR GAP

A minor gap is an isolated issue that does not cause a breakdown in operations or affect the ability of the business to meet its objectives. However, it signals a weakness in processes or procedures that, if left unresolved or recurring, could escalate into a major nonconformance.

- Examples: Missing training records, invoicing mistakes, improperly calibrated machines.
- Impact: Does not affect certification directly but must be corrected within a specified time frame to avoid escalation.

OBSERVATIONS/OPPORTUNITY FOR IMPROVEMENT

An observation is a suggestion made to enhance the effectiveness of the ISMS. While no nonconformance is identified, observations highlight areas where improvements could prevent future issues or strengthen controls.

- Examples: Considerations to prevent potential nonconformities, instances where ISMS requirements are met but further improvements are suggested, or areas where insufficient evidence suggests a need for enhanced controls.
- Impact: Does not affect certification but serves as an opportunity for proactive improvement and risk mitigation.

Note:

The audit is sample based; therefore, the absence of raised non-conformities does not imply that non-conformities are not present in the processes.

POSITIVES

1. The organisation has shown enthusiasm towards the implementation of the ISMS.
2. The auditees demonstrated transparency and accountability in their responsible areas of expertise.
3. The employee contracts are well very documented with the necessary information security clauses referenced.
4. OMS has shown enthusiasm towards the implementation of the Information Security Management System.
5. The audit team received full cooperation from all stakeholders.

COMMENTARY AND SUMMARIES

Information Security Management System – Management Controls

Clause 4: Context of the Organization

OMS has identified both internal and external issues through a SWOT and PESTEL analysis that are relevant to its purpose and that impact its ability to achieve the intended outcomes of its ISMS. The organisation has also identified the interested parties relevant to the ISMS, along with their applicable requirements concerning information security. However, OMS has not yet defined the boundaries and applicability of the ISMS to establish its scope, nor has it determined the interfaces and dependencies between its various activities. Additionally, the organisation has not established or implemented the ISMS in line with the requirements of the standard. Top management has not yet set an information security policy or defined information security objectives. Furthermore, the ISMS requirements have not been integrated into the organisation's processes, and top management has not ensured that the ISMS is positioned to achieve its intended outcomes.

Clause 5: Leadership

Top management has not yet established an information security policy or defined the information security objectives. There is no evidence that the ISMS requirements have been integrated into the organisation's processes, nor that top management has ensured the ISMS achieves its intended outcomes. Responsibilities and authorities for roles relevant to information security have not been assigned or communicated. The responsibility and authority to ensure the ISMS conforms to the requirements of ISO/IEC 27001:2022 have not been allocated, and no one has been tasked with reporting on the performance of the ISMS to top management.

Clause 6: Planning

When planning for the ISMS, OMS has not taken into account the issues identified in Clause 4.1 or the requirements of interested parties outlined in Clause 4.2. As a result, the organisation has not determined the risks and opportunities that need to be addressed to ensure the ISMS achieves its intended outcomes. OMS has not considered how to prevent or reduce undesired effects, nor has it addressed how to achieve continual improvement. There is no evidence of planned actions to address identified risks and opportunities, nor of how these actions would be integrated into ISMS processes. Additionally, OMS has not planned how to evaluate the effectiveness of such actions. The organisation has also not defined or applied an information security risk treatment process, and information security objectives have not been established.

Clause 7: Support

OMS has provided the necessary resources for the establishment, implementation, maintenance, and continual improvement of its ISMS. The organisation has also identified the required competence for individuals performing work that affects information security performance and has ensured that employees are competent based on their education, training, and experience. Actions have been taken to acquire the necessary competence and to evaluate their effectiveness. However, OMS has not consistently retained documented evidence of competence, and job descriptions for some employees are still outstanding.

Although an information security policy has not yet been established, OMS has conducted awareness training on the ISO/IEC 27001:2022 standard for all employees. The organisation has not determined the need for internal and external communications related to the ISMS. There is no clarity on what should be communicated, when, with whom, by whom, or through which processes communication should occur.

OMS does not yet maintain documented information in accordance with the ISMS requirements. When creating and updating documentation, appropriate identification, description, format, media, and timing for review and approval have not been ensured. Additionally, key processes such as the distribution, access, retrieval, classification, and use of documented information are yet to be defined. The storage, preservation, retention, and disposal of hard copy records have not been established. Finally, documented information of external origin necessary for ISMS planning and operations has not been appropriately identified or controlled.

Clause 8: Operations

OMS has not planned or implemented the processes required to meet its information security objectives. There are no implemented plans in place to achieve the objectives outlined in Clause 6.2.

While the organisation is maintaining some documented information to demonstrate that certain processes have been carried out, it has not established controls for planned changes or reviewed the impact of unintended changes. Outsourced processes have been identified and are being managed appropriately. However, OMS has not yet conducted information security risk assessments at planned intervals in line with the requirements of the standard. Furthermore, the organisation does not retain documented information on the results of these risk assessments or on the outcomes of its risk treatment activities.

Clause 9: Performance Evaluation

OMS is not currently evaluating the performance of its ISMS or its overall effectiveness. The organisation has not determined what needs to be monitored and measured, including its information security processes and controls. Methods for monitoring, measurement, analysis, and evaluation have not been defined to ensure valid results. OMS has also not established when monitoring and measurement should take place, who is responsible for carrying it out, or when and by whom the results should be analysed and evaluated. As a result, there is no documented evidence retained for monitoring and measurement activities.

Internal audits are not being conducted at planned intervals to assess whether the ISMS conforms to either the organisation's own requirements or those of the ISO/IEC 27001:2022 standard. An audit programme has not been planned, established, implemented, or maintained. Audit criteria and scope have not been defined, and auditors have not been selected in a way that ensures objectivity and impartiality. The process for reporting audit results to relevant management has not been clarified or documented. OMS has not retained documented information related to audit programmes or results, and no internal audits have been performed to date. Furthermore, a management review that meets the requirements of the standard has not been established, presented, documented, or minuted.

Clause 10: Continual improvement

WWISE is conducting a gap assessment for the first time on behalf of OMS. Prior to this assessment, no non-conformities had been identified or raised.

Annexure A Summaries

The gap assessment highlighted several areas where the OMS shows potential for further alignment with the ISO/IEC 27001:2022 standard. Several foundational elements have been established, various clauses and controls present opportunities for improvement in terms of documentation, implementation consistency, and operational maturity.

Key documentation such as access control, supplier management, cryptographic (Encryption) controls, and information security policies are not yet formally documented. Processes are being managed informally, which do not fully support operational consistency across the organisation.

Awareness and training initiatives have been identified, the delivery and frequency of such programs vary, and not all staff members have yet received structured information security training.

The organisation is managing asset inventories, access provisioning, and change control on a day-to-day basis; however, these activities are not always supported by detailed procedures or formal tracking mechanisms. User account management, privilege allocation, and deactivation of access following role changes or terminations are being handled, though the processes differ across departments and are not consistently supported by documented workflows.

Event logging, user activity monitoring, and audit log management are being considered but are not uniformly implemented across all systems or environments. Controls related to secure disposal of media, use of cryptographic techniques, and protection of transmitted information are pending standardization. Information transfer methods, including email, shared platforms, and physical media, are used operationally, but are not always be governed by a clear policy.

Supplier and third-party management practices are being carried out as part of procurement and operational activities. While engagement with suppliers is actively maintained, security-specific requirements in contracts, onboarding, and ongoing evaluation are still being developed. Similarly, risk assessments specific to supplier services or data access are not always performed in a formal or documented manner.

Incident management has been addressed through informal or ad-hoc reporting channels, with some internal escalation practices in place. However, a structured approach to logging, investigating, documenting, and reviewing security incidents is currently being developed.

The organisation has begun to examine its approach to backups, disaster recovery, and business continuity, with certain practices in place, though comprehensive documentation and testing procedures are still maturing. Additional areas such as secure development practices, system acquisition and testing, capacity planning, and operational change control reflect varying levels of maturity, with some being handled through general IT processes rather than dedicated information security procedures.

Overall, the organisation displays a positive orientation toward strengthening its information security posture. Efforts are underway across multiple domains to develop, document, and standardize practices in support of the ISO/IEC 27001:2022 framework. The ongoing activities observed during the assessment suggest a commitment to continuous improvement, with internal discussions and actions already taking place to formalise and enhance the ISMS.

NON-CONFORMITIES

No	GAPS	AREA	CLAUSE	CLASS
1	OMS has not determined the boundaries and applicability of the information security management system to establish its scope.	ISMS	4.3	System GAP
2	The organisation has also not determined the interfaces and dependencies between activities conducted by the organisation.	ISMS	4.3(c)	System GAP
3	OMS has not established and implemented an Information Security Management System in accordance with the requirements of the standard.	ISMS	4.4	System GAP
4	Top management has not yet established an information security policy and the information security objectives.	ISMS	5.1, 5.3, 6.2	System GAP
5	Top management has not ensured the integration of the Information Security Management System requirements into the organisation's processes and that the Information Security Management System achieves its intended outcomes.	ISMS	5.1	System GAP
6	Top management has not ensured that the responsibilities and authorities for roles relevant to information security are assigned and communicated.	ISMS	5.3	System GAP
7	Top management has not assigned the responsibilities and authorities to ensure that the Information Security Management System conforms to the requirements of ISO/IEC 27001:2022.	ISMS	5.3	System GAP
8	Top management has not assigned the responsibility and authority for reporting on the performance of the Information Security Management System to top management.	ISMS	5.3	System GAP
9	When planning for the Information Security Management System, OMS has not considered the issues referred to in 4.1 and the requirements referred to in 4.2 and determined the risks and opportunities that need to be addressed to ensure that the Information Security Management System can achieve its intended outcome.	ISMS	6.1	System GAP
10	When planning for the Information Security Management System, OMS has not considered the issues referred to in 4.1 and the requirements referred to in 4.2 and determined the risks and opportunities that need to be addressed to prevent, or reduce, undesired effects.	ISMS	6.1.1	System GAP
11	When planning for the Information Security Management System, OMS has not considered the issues referred to in 4.1 and the requirements referred to in 4.2 and determined the risks and opportunities that need to be addressed to achieve continual improvement.	ISMS	6.1.1	System GAP
12	OMS has not planned for actions to address risks and opportunities.	ISMS	6.1.1	System GAP
13	OMS has not planned for actions on how to integrate and implement the actions into its information security management system processes.	ISMS	6.1.1	System GAP

14	OMS has not effectively planned to evaluate the effectiveness of actions to address risks.	ISMS	6.1.1	System Gap
15	OMS has not defined or applied an information security risk treatment process.	ISMS	6.1.2, 6.1.3	System Gap
16	OMS has not determined the need for internal and external communications relevant to the Information Security Management System including what to communicate, when to communicate, with whom to communicate, who shall communicate, and the process required for said communication.	ISMS	7.4	System Gap
17	OMS does not have documented information in terms of an Information Security Management System.	ISMS	7.5.1	System Gap
18	When creating and updating documented information, OMS has not ensured appropriate identification and description, format and media, or appropriate times as to when the reviewing and approval on the suitability and adequacy of the documented information will take place.	ISMS	7.5.2	System Gap
19	The organisation has not planned or implemented the processes needed to meet and achieve information security objectives.	ISMS	8.1	System Gap
20	OMS is not controlling planned changes or reviewing the consequences of unintended changes.	ISMS	8.1	System Gap
21	OMS has not yet performed information security risk assessments at planned intervals as per the requirements of the standard.	ISMS	8.2, 8.3	System Gap
22	OMS is not evaluating the information security performance and the effectiveness of the Information Security Management System.	ISMS	9.1	System Gap
23	OMS has not determined what needs to be monitored and measured (including information security processes and controls), methods for monitoring, measurement, analysis, and evaluation, when the monitoring and measuring shall be performed, who shall monitor and measure, or when the results from monitoring and measurement shall be analysed and evaluated. As a result, there is no documentation pertaining this.	ISMS	9.1	System Gap
24	OMS is not conducting internal audits at planned intervals to provide information on whether the Information Security Management System conforms to the organisation's own requirements for its Information Security Management System.	ISMS	9.2	System Gap
25	OMS has not planned, established, implemented, and is not maintaining an audit programmes, including the frequency, methods, responsibilities, planning requirements and reporting.	ISMS	9.2	System Gap
26	OMS has not yet documented the information security policies as required by the requirements of the standard. No communication of current IS policies and approval could be verified at the time of audit.	ICT Operations and Governance	A.5.1	System GAP
27	Responsibilities for carrying out specific security processes have not been clearly identified, defined and communicated to the relevant parties or appointed ISO champions within the different units or department.	ICT Operations and Governance	A.5.2	System GAP
28	There is no process in place to mitigate potential attacks and harmful events.	ICT Operations and Governance	A.5.7	System GAP
29	There is no policy governing information classification.	ICT Operations and Governance	A.5.12	System GAP

30	The process of labelling assets and information has not been finalized and communicated within the organization to ensure consistency throughout OMS.	Finance	A.5.13	System GAP
31	There is no policy in place to govern how information is transferred.	ICT Operations and Governance	A.5.14	System GAP
32	There is no role-based access control in place that is documented.	ICT Operations and Governance	A.5.15	System GAP
33	There are shared credentials from some of the systems internally such as Umami, Contabo Server & Domains.co.za & CUpa	Finance & ICT Operations and Governance	A.5.16	System GAP
34	Access rights are not controlled and reviewed.	ICT Operations and Governance	A.5.18	System GAP
35	There is no documented process in place to review current suppliers.	ICT Operations and Governance	A.5.22	System GAP
36	All the cloud service providers sourced do not follow a formal onboarding process.	ICT Operations and Governance	A.5.23	System GAP
37	There is no incident management processes.	ICT Operations and Governance	A.5.24	System GAP
38	There is no process to ensure information security events are properly assessed and classified	ICT Operations and Governance	A.5.25	System GAP
39	There is no incident response plan.	ICT Operations and Governance	A.5.26	System GAP
40	Organization's security function have not been documented, implemented and maintained	ICT Operations and Governance	A.5.29	System GAP
41	ICT readiness for business continuity is not planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	ICT Operations and Governance	A.5.30	System GAP
42	There is no process for reporting of identified information security weakness	ICT Operations and Governance	A.6.8	System GAP
43	Clear Desk and Clear Desk Policy has not been implemented.	ICT Operations and Governance	A.7.7	System GAP
44	Observations revealed lack of maintenance in the server room, characterized by general housekeeping practices, including no cable management, and the presence of access boxes. Furthermore, assets lack proper labelling which were identified within the rack.	ICT Operations and Governance	A.7.8	System GAP
45	There is no access control policy or reviews in-house that have been conducted to manage which users have access to certain systems.	ICT Operations and Governance	A.8.3	System GAP
46	Pseudonymization (Replacing identifying fields in a dataset with artificial identifiers or pseudonyms (e.g., replacing a name with a user ID or code), anonymization (transforming personal data so that individuals cannot be identified), salting techniques (Adding a random value (salt) to data before hashing it to make the result unique) have not been standardized and deployed.	ICT Operations and Governance	A.8.11	System GAP
47	Data Leakage Prevention requirements of ISO/IEC 27002:2022 have not been defined and implemented.	ICT Operations and Governance	A.8.12	System GAP
48	There is no network management process in place	ICT Operations	A.8.20	System

		and Governance		GAP
49	Websites such as uTorrent, adult content, and gambling sites can be accessed. Malicious software can be downloaded on the LAN and WAN.	ICT Operations and Governance	A.8.23	System GAP
50	There is no encryption method that is utilized internally such as BitLocker.	ICT Operations and Governance	A.8.24	System GAP
51	There are established Policies and procedures in place within OMS, however they need to be document controlled and reviewed according to the control of document procedure.	ISMS	A.5.4	System GAP
52	There is no documented procedure for contact with relevant authorities (law enforcement etc.)	ISMS	A.5.5	System GAP
53	Individuals within OMS do not maintain active memberships in relevant special interest groups.	ISMS	A.5.6	Process Gap
54	Information security requirements are not specified when new systems are introduced.	ICT Operations and Governance	A.5.8	Process Gap
55	There is no acceptable use form established for handing out assets to employees.	Finance & ICT Operations and Governance	A.5.10	Process Gap
56	OMS do not have a process defined to control the return of assets upon termination of employment and that process has not been formally documented and communicated.	Finance	A.5.11	Process Gap
57	There is no formal policy defined to implement MFA and the organization has not effectively defined and documented a password policy.	ICT Operations and Governance	A.5.17	Process Gap
58	There is no clause in the supplier contracts that govern or manage how appropriate technical and organizational measures are implemented to ensure the confidentiality, integrity, and availability of client data, including compliance with ISO/IEC 27001 controls	ISMS	A.5.19	Process Gap
59	There is no formal process for logging issues/incidents within OMS.	ICT Operations and Governance	A.5.27	
60	There is no system in place that manages the collection of evidence to use as records in an event of an incident.	ICT Operations and Governance	A.5.28	Process Gap
61	At the time of the GAP we could not verify of OMS has licensed any of their Intellectual property rights including software or document copyright, design rights, trademarks, patents and source code licenses.	ICT Operations and Governance	A.5.32	Process Gap
62	OMS keeps record of all intellectual property rights and use of proprietary software products. The initiative of managing the records has been established, however not effectively followed throughout the organization. There is no retention of policy that governs how long information should be retained for internally.	ICT Operations and Governance	A.5.33	Process Gap
63	OMS has not conducted an independent review of their information security controls as per the standard. People, processes and technologies are not reviewed independently at planned intervals.	ICT Operations and Governance	A.5.35	Process Gap
64	OMS do not have a documented process for terminating or changing employment duties.	ICT Operations and Governance	A.6.5	Process Gap
65	Entrance area at OMS has suitable entry control systems to ensure only authorised personnel have access. However, there is no access control system at the front reception to manage access within the OMS office. There is no visitor logbook to manage access within OMS office.	ICT Operations and Governance	A.7.2	Process GAP
66	There is no process in place to monitor the physical security measures used to protect the personnel and property for OMS.	ICT Operations and Governance	A.7.4	Process GAP

67	There is no policy covering security assets off-site.	ICT Operations and Governance	A.7.9	Process Gap
68	There is no policy that governs removable media.	ICT Operations and Governance	A.7.10	Process Gap
69	There is no UPS onsite for the cabinet	ICT Operations and Governance	A.7.11	Process Gap
70	There is a cabinet housing critical data/network infrastructure of the organization, however the cables are not labeled to specify which cables are the Uplink (Lan) or WAN link from the ONT.	ICT Operations and Governance	A.7.12	Process Gap
71	There is no policy covering how information assets may be reused.	ICT Operations and Governance	A.7.14	Process Gap
72	Privileged access accounts are not separately managed and controlled.	ICT Operations and Governance	A.8.2	Process Gap
73	OMS makes use of MFA on some of their internal System. In systems that are using a shared account there Is no MFA configured.	ICT Operations and Governance	A.8.5	Process Gap
74	There is a system called Beszel that handles capacity management, monitors containers and servers for OBSE production. Thresholds for capacity alerts for CPU and average load are not documented and configured to be triggered by excessive use of CPU usage, Memory and disk usage.	ICT Operations and Governance	A.8.6	Process Gap
75	Information deletion is addressed as and when it comes. User machines are wiped before they are handed over to the next employee. There is no official method of disposing of information on old assets that are not being utilized by employees.	ICT Operations and Governance	A.8.10	Process Gap
76	There is a repository outside of GitHub called Gitea - this server mirrors the application. Coolify backups to self-hosted server. (1 server is hosted is in Germany) and another is USA (Newark). Other backups are running from user SharePoint and one drive. However, there is no documented backup policy.	ICT Operations and Governance	A.8.13	Process Gap
77	There are no formal monitoring methods that have been conducted to monitor anomalous behavior in the OMS's Infrastructure.	ICT Operations and Governance	A.8.16	Process Gap
79	There is no NTP (Network Time Protocol) server that endpoints and devices on the domain and Network synchronize to.	ICT Operations and Governance	A.8.17	Process Gap
80	There is no process in place to control the installation of software onto operational systems.	ICT Operations and Governance	A.8.19	
81	Presently, there are no authentication controls in place for accessing administrative network controls within the organization. Moreover, the system logs (sys logs) and event logs are not currently reviewed or monitored within the organisation.	ICT Operations and Governance	A.8.21	Process Gap
82	There are no documented principles on how systems must be engineered to ensure security.	ICT Operations and Governance	A.8.27	Process Gap
83	There is no process to accept new systems/applications or upgrades, into production use.	ICT Operations and Governance	A.8.29	Process Gap
84	There is no change control procedure and process are Fin placed at OMS.	ICT Operations and Governance	A.8.32	Process Gap
85	OMS has not retained appropriate documented information as evidence	ISMS	7.2	

	of competence consistently. Job descriptions for some employees have not been created.			Process Gap
86	The distribution, access, retrieval, classification and use of documented information is yet to be defined. The storage, preservation, retention, and disposition of hard copies are yet to be established. Documented information of external origin, determined by OMS to be necessary for the planning and operation of the Information Security Management System, has not been identified as appropriate, and controlled.	ISMS	7.5.3	Process Gap

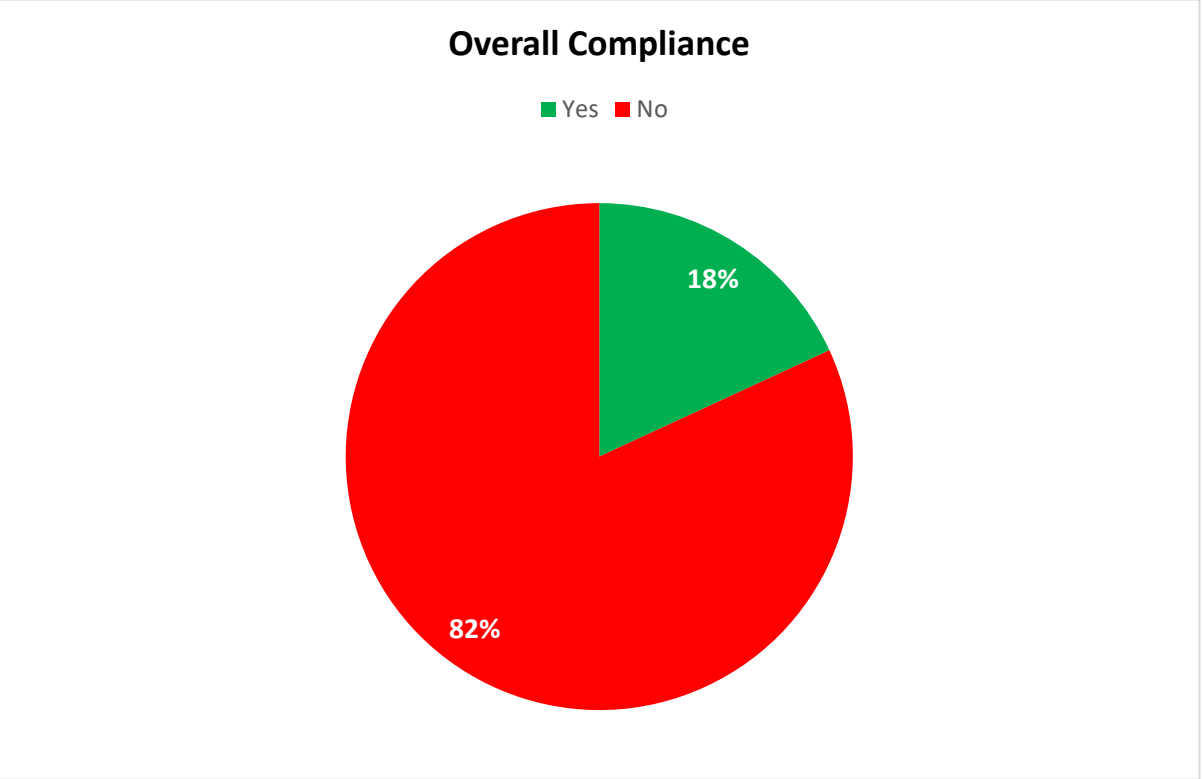


Figure 1:

The pie chart above shows the conformance status to the ISO/IEC 27001:2022 standard of **18%** and non-conformances at **82%**. This can be justified with the audit checklist below on each control of the requirements of the standard.

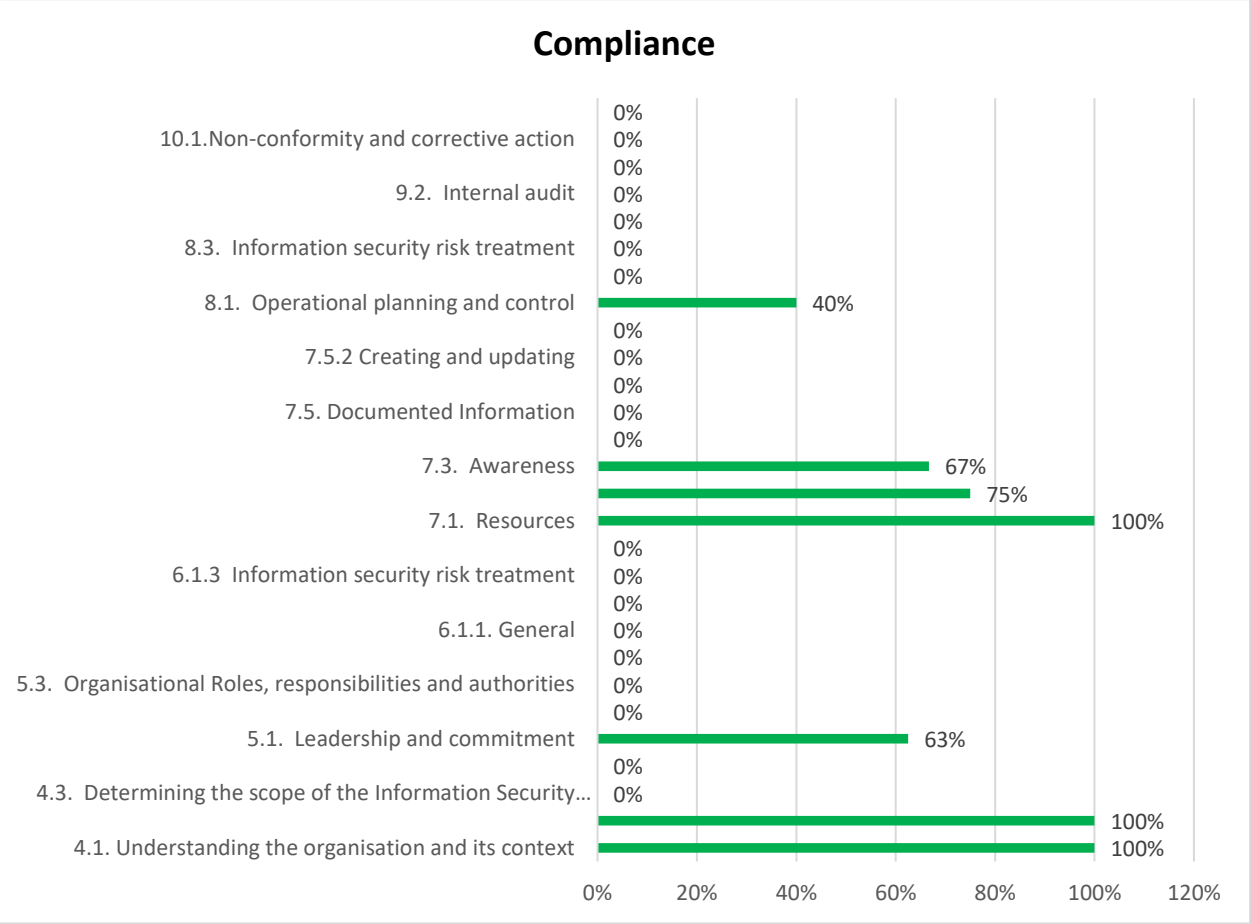


Figure 2:

The bar chart above shows the conformance status to the ISO/IEC 27001:2022 standard based onmanagement controls.

Clause No.	ISO 27001 Clause Questionnaire	Compliance (Yes/No)	NCR / Observation	Comments
4	**Context of the Organization**			
4.1.	**Understanding Owethu Managed Services (Pty) Ltd and its context**			
	Has the organization determined external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcomes of its Information Security Management System?	Yes	N/A	OMS has determined internal and external (SWOT Analysis) issues that are relevant to its purpose and that affect its ability to achieve the intended outcome of its Information Security Management System.
4.2.	**Understanding the needs and expectations of interested parties**			
	Has the organization determined: a) interested parties that are relevant to the Information Security Management System?	Yes	N/A	OMS has determined the interested parties that are relevant to the Information Security Management System.
	b) the requirements of these interested parties relevant to information security?	Yes	N/A	The organisation has determined the interested parties' requirements that are relevant to information security.
4.3.	**Determining the scope of the Information Security Management System**			
	Has the organization determined the boundaries and applicability of the information security management system to establish its scope?	No	Major NCR	OMS has not determined the boundaries and applicability of the information security management system to establish its scope. The organisation has also not determined the interfaces and dependencies between activities conducted by the organisation.
	When determining this scope, has the organization considered: a) the external and internal issues referred to in 4.1?	No	Major NCR	
	b) the requirements referred to in 4.2?	No	Major NCR	

	c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations?	No	Major NCR	
	Is the scope available as documented information?	No	Major NCR	
4.4.	**Information Security Management System**			
	Has the organization established, implemented, and is maintaining and continually improving an Information Security Management System, in accordance with the requirements of this International Standard?	No	Major NCR	OMS has not established and implemented an Information Security Management System in accordance with the requirements of the standard.
5	**Leadership**			
5.1.	**Leadership and commitment**			
	Has top management demonstrated leadership and commitment with respect to the Information Security Management System by: a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization?	No	Major NCR	Top management has not yet established an information security policy and the information security objectives. Top management has also not ensured the integration of the Information Security Management System requirements into the organisation's processes and that the Information Security Management System achieves its intended outcomes.

	b) ensuring the integration of the Information Security Management System requirements into the organization's processes?	No	Minor NCR	
	c) ensuring that the resources needed for the Information Security Management System are available?	Yes	N/A	
	d) communicating the importance of effective information security management and of conforming to the Information Security Management System requirements?	Yes	N/A	

	e) ensuring that the Information Security Management System achieves its intended outcomes?	No	Minor NCR	
	f) directing and supporting persons to contribute to the effectiveness of the Information Security Management System?	Yes	N/A	
	g) promoting continual improvement?	Yes	N/A	
	h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility?	Yes	N/A	
5.2.	**Policy**			
	Has the top management established an information security policy that: a) is appropriate to the purpose of the organization?	No	Major NCR	Top management has not established an information security policy.

	b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives?	No	Major NCR	
	c) includes a commitment to satisfy applicable requirements related to information security?	No	Major NCR	
	d) includes a commitment to continual improvement of the Information Security Management System?	No	Major NCR	
	Is the information security policy: a) available as documented information?	No	Major NCR	
	b) communicated within the organization?	No	Major NCR	
	c) available to interested parties, as appropriate?	No	Major NCR	
5.3.	**Organisational Roles, responsibilities and authorities**			
	Has the top management ensured that the responsibilities and authorities for roles relevant to information security are assigned and communicated?	No	Major NCR	Top management has not ensured that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

	Has the top management assigned the responsibility and authority for: a) ensuring that the Information Security Management System conforms to the requirements of this International Standard?	No	Major NCR	Top management has not assigned the responsibilities and authorities to ensure that the Information Security Management System conforms to the requirements of ISO/IEC 27001:2022.
	b) reporting on the performance of the Information Security Management System to top management?	No	Major NCR	Top management has not assigned the responsibility and authority for reporting on the performance of the Information Security Management System to top management.
6	**Planning**			
6.1.	**Actions to address risks and opportunities.**			
6.1.1.	**General**			
	When planning for the Information Security Management System, has the organization considered the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a) ensure the Information Security Management System can achieve its intended outcomes?	No	Major NCR	When planning for the Information Security Management System, OMS has not considered the issues referred to in 4.1 and the requirements referred to in 4.2 and determined the risks and opportunities that need to be addressed to ensure that the Information Security Management System can achieve its intended outcome.
	b) prevent, or reduce, undesired effects?	No	Major NCR	OMS has not considered how to prevent, or reduce, undesired effects.
	c) achieve continual improvement?	No	Major NCR	OMS has not considered achieving continual improvement.
	Has the organization planned: a) actions to address these risks and opportunities?	No	Major NCR	OMS has not planned for actions to address risks and opportunities.
	b) how to 1) integrate and implement the actions into its information security management system processes?	No	Major NCR	OMS has not planned for actions on how to integrate and implement the actions into its information security management system processes.

	2) evaluate the effectiveness of these actions?	No	Major NCR	OMS has not effectively planned to evaluate the effectiveness of actions to address risks.
6.1.2.	**Information security risk assessment**			
	Has the organization defined and applied an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria?	No	Major NCR	OMS has not defined or applied an information security risk treatment process.
	2) criteria for performing information security risk assessments?	No	Major NCR	
	b) ensures that repeated information security risk assessments produce consistent, valid and comparable results?	No	Major NCR	
	c) identifies the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the Information Security Management System?	No	Major NCR	
	2) identify the risk owners?	No	Major NCR	
	d) analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize?	No	Major NCR	
	2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1)?	No	Major NCR	

	3) determine the levels of risk?	No	Major NCR	
	e) evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a)?	No	Major NCR	
	2) prioritize the analysed risks for risk treatment?	No	Major NCR	
	Does the organization retain documented information about the information security risk assessment process?	No	Major NCR	
6.1.3	**Information security risk treatment**			
	Has the organization defined and applied an information security risk treatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results?	No	Major NCR	OMS has not defined or applied an information security risk treatment process.
	b) determine all controls that are necessary to implement the information security risk treatment options chosen?	No	Major NCR	
	c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted?	No	Major NCR	

	d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A?	No	Major NCR	
	e) formulate an information security risk treatment plan?	No	Major NCR	
	f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks?	No	Major NCR	
	Does the organization retain documented information about the information security risk treatment process?	No	Major NCR	
6.2.	**Information Security objectives and plan to achieve them**			
	Has the organization established information security objectives at relevant functions and levels?	No	Major NCR	OMS has not established information security objectives.
	Are the information security objectives: a) consistent with the information security policy?	No	Major NCR	
	b) measurable (if practicable)?	No	Major NCR	
	c) taking into account applicable information security requirements, and results from risk assessment and risk treatment?	No	Major NCR	
	d) communicated?	No	Major NCR	
	e) updated as appropriate?	No	Major NCR	
	Does the organization retain documented information on the information security objectives?	No	Major NCR	

	When planning how to achieve its information security objectives, has the organization determined: a) what will be done?	No	Major NCR	
	b) what resources will be required?	No	Major NCR	
	c) who will be responsible?	No	Major NCR	
	d) when it will be completed?	No	Major NCR	
	e) how the results will be evaluated?	No	Major NCR	
7	**Support**			
7.1.	**Resources**			
	Has the organization determined and provided the resources needed for the establishment, implementation, maintenance and continual improvement of the Information Security Management System?	Yes	N/A	OMS has determined and provided the resources needed for the establishment, implementation, maintenance, and continual improvement of the Information Security Management System.
7.2.	**Competence**			
	Has the organization: a) determined the necessary competence of persons doing work under its control that affects its information security performance?	Yes	N/A	OMS has determined the necessary competence of the people doing work under its control that affects its information security performance.
	b) ensured that these persons are competent on the basis of appropriate education, training, or experience?	Yes	N/A	OMS has ensured that the employees are competent on the basis of appropriate education, training, and experience.
	c) where applicable, taken actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken?	Yes	N/A	OMS has taken actions to acquire the necessary competence and evaluate the effectiveness of the actions taken.
	d) retained appropriate documented information as evidence of competence?	No	Minor NCR	OMS has not retained appropriate documented information as evidence of competence consistently. Job descriptions

				for some employees have not been created.
7.3.	**Awareness**			
	Are the persons doing work under the organization's control aware of: a) the information security policy?	No	Major NCR	Although OMS does not have an information security policy, awareness training on the ISO/IEC 27001:2022 standard was conducted for all employees.
	b) their contribution to the effectiveness of the Information Security Management System, including the benefits of improved information security performance?	Yes	N/A	
	c) the implications of not conforming with the Information Security Management System requirements?	Yes	N/A	
7.4.	**Communication**			
	Has the organization determined the need for internal and external communications relevant to the Information Security Management System including: a) on what to communicate?	No	Major NCR	OMS has not determined the need for internal and external communications relevant to the Information Security Management System including what to communicate.
	b) when to communicate?	No	Major NCR	OMS has not defined when to communicate.
	c) with whom to communicate?	No	Major NCR	OMS has not defined with whom to communicate.
	d) who shall communicate?	No	Major NCR	OMS has not defined who shall communicate.

	e) the processes by which communication shall be effected?	No	Major NCR	OMS has not defined the processes by which communication shall be effective.
7.5.	**Documented Information**			
7.5.1	**General**			
	Does the organization's Information Security Management System include: a) documented information required by this International Standard?	No	Major NCR	OMS does not have documented information in terms of an Information Security Management System.
	b) documented information determined by the organization as being necessary for the effectiveness of the Information Security Management System?	No	Minor NCR	
7.5.2	**Creating and updating**			
	When creating and updating documented information, has the organization ensured appropriate: a) identification and description (e.g. a title, date, author, or reference number)?	No	Major NCR	When creating and updating documented information, OMS has not ensured appropriate identification and description, format and media, or appropriate times as to when the reviewing and approval on the suitability and adequacy of the documented information will take place.
	b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic)?	No	Major NCR	
	c) review and approval for suitability and adequacy?	No	Major NCR	
7.5.3	**Control of documented information**			

	Is the documented information required by the Information Security Management System and by this International Standard controlled to ensure: a) it is available and suitable for use, where and when it is needed; and b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity)?	No	Minor NCR	The distribution, access, retrieval, classification and use of documented information is yet to be defined. The storage, preservation, retention, and disposition of hard copies are yet to be established. Documented information of external origin, determined by OMS to be necessary for the planning and operation of the Information Security Management System, has not been identified as appropriate, and controlled.
	For the control of documented information, has the organization addressed the following activities, as applicable: a) distribution, access, retrieval and use?	No	Minor NCR	
	b) storage and preservation, including the preservation of legibility; e) control of changes (e.g. version control)?	No	Minor NCR	
	c) retention and disposition?	No	Minor NCR	
	Has the documented information of external origin, determined by the organization to be necessary for the planning and operation of the Information Security Management System, been identified as appropriate, and controlled?	No	Minor NCR	
8	**Operations**			
8.1.	**Operational planning and control**			
	Has the organization planned, implemented and is controlling the processes needed to meet information security requirements, and to implement the actions determined in 6.1?	No	Major NCR	The organisation has not planned or implemented the processes needed to meet information security objectives.

	Has the organization also implemented plans to achieve information security objectives determined in 6.2?	No	Major NCR	The organisation has not implemented plans to achieve information security objectives determined in 6.2.
	Is the organization keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned?	Yes	N/A	The organisation is keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned.
	Is the organization controlling planned changes and reviewing the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary?	No	Major NCR	OMS is not controlling planned changes or reviewing the consequences of unintended changes.
	Is the organization ensuring that outsourced processes are determined and controlled?	Yes	N/A	OMS ensures that outsourced processes are determined and controlled.
8.2.	**Information security risk assessment**			
	Is the organization performing information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a)?	No	Major NCR	OMS has not yet performed information security risk assessments at planned intervals as per the requirements of the standard.
	Is the organization retaining documented information of the results of the information security risk assessments?	No	Major NCR	OMS is not retaining documented information on the results of the information security risk assessments.
8.3.	**Information security risk treatment**			
	Is the organization implementing the information security risk treatment plan?	No	Major NCR	OMS has not yet performed information security risk assessments at planned intervals as per the requirements of the standard.

	Is the organization retaining documented information of the results of the information security risk treatment?	No	Major NCR	OMS is not retaining documented information on the results of the information security risk treatment.
9	**Performance Evaluation**			
9.1.	**Monitoring, measurement, analysis and evaluation**			
	Is the organization evaluating the information security performance and the effectiveness of the Information Security Management System?	No	Major NCR	OMS is not evaluating the information security performance and the effectiveness of the Information Security Management System.
	Has the organization determined: a) what needs to be monitored and measured, including information security processes and controls?	No	Major NCR	OMS has not determined what needs to be monitored and measured, including information security processes and controls.
	b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results?	No	Major NCR	OMS has not determined the methods for monitoring, measurement, analysis, and evaluation, as applicable, to ensure valid results.
	c) when the monitoring and measuring shall be performed?	No	Major NCR	OMS has not determined when the monitoring and measuring shall be performed.
	d) who shall monitor and measure?	No	Major NCR	OMS has not determined who shall monitor and measure.
	e) when the results from monitoring and measurement shall be analysed and evaluated?	No	Major NCR	OMS has not determined when the results from monitoring and measurement shall be analysed and evaluated.
	f) who shall analyse and evaluate these results?	No	Major NCR	OMS has not determined who shall analyse and evaluate these results.
	Is the organization retaining appropriate documented information as evidence of the monitoring and measurement results?	No	Major NCR	OMS is not retaining appropriate documented information as evidence of the monitoring and measurement results.

9.2.	Internal audit			
	Is the organization conducting internal audits at planned intervals to provide information on whether the Information Security Management System: a) conforms to: 1) the organization's own requirements for its Information Security Management System?	No	Major NCR	OMS is not conducting internal audits at planned intervals to provide information on whether the Information Security Management System conforms to the organisation's own requirements for its Information Security Management System.
	2) the requirements of this International Standard?	No	Major NCR	OMS is not conducting internal audits at planned intervals to provide information on whether the Information Security Management System conforms to the international standard's requirements for the Information Security Management System.
	b) is effectively implemented and maintained?	No	Major NCR	OMS is not conducting internal audits at planned intervals to provide information on whether the Information Security Management System conforms to the organisation's own requirements for its Information Security Management System.
	Has the organization: a) planned, established, implemented and is maintaining audit programmes, including the frequency, methods, responsibilities, planning requirements and reporting?	No	Major NCR	OMS has not planned, established, implemented, and is not maintaining an audit programme, including the frequency, methods, responsibilities, planning requirements and reporting.
	b) defined the audit criteria and scope for each audit?	No	Major NCR	OMS has not defined the audit criteria and scope for each audit.
	c) selected auditors and conducted audits that ensure objectivity and the impartiality of the audit process?	No	Major NCR	OMS has not selected auditors and conducted audits that ensure objectivity

				and the impartiality of the audit process.
	d) ensured that the results of the audits are reported to relevant management?	No	Major NCR	OMS has not ensured that the results of the audits are reported to relevant management. Some controls are not reported to relevant management as these controls are considered adequate, this process has, however, not been clarified and documented.
	e) retained documented information as evidence of the audit programmes and the audit results?	No	Major NCR	OMS has not retained documented information as evidence of the audit programmes and the audit results.
	Is the audit programmes taking into consideration the importance of the processes concerned and the results of previous audits?	No	Major NCR	OMS has not conducted any internal audits.
9.3.	**Management Review**			
	Does the top management review the organization's Information Security Management System at planned intervals to ensure its continuing suitability, adequacy and effectiveness?	No	Major NCR	A management review in line with the standards requirements has not been established, presented, documented, or minuted.
	Does the management review include consideration of: a) the status of actions from previous management reviews?	No	Major NCR	
	b) changes in external and internal issues that are relevant to the Information Security Management System?	No	Major NCR	
	c) feedback on the information security performance, including trends in: 1) nonconformities and corrective actions?	No	Major NCR	
	2) monitoring and measurement results?	No	Major NCR	

	3) audit results?	No	Major NCR	
	4) fulfilment of information security objectives?	No	Major NCR	
	d) feedback from interested parties?	No	Major NCR	
	e) results of risk assessment and status of risk treatment plan?	No	Major NCR	
	f) opportunities for continual improvement?	No	Major NCR	
	Do the outputs of the management review include decisions related to continual improvement opportunities and any needs for changes to the Information Security Management System?	No	Major NCR	
	Does the organization retain documented information as evidence of the results of management reviews?	No	Major NCR	
10	**Improvement**			
10.1.	**Non-conformity and corrective action**			
	When a nonconformity occurs, does the organization: a) react to the nonconformity, and as applicable: 1) take action to control and correct it?	Yes	Observation	WWISE is conducting a gap assessment for the first time on behalf of OMS. No non-conformities have been raised prior to the gap assessment.
	2) deal with the consequences?	Yes	Observation	
	b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity?	Yes	Observation	
	2) determining the causes of the nonconformity?	Yes	Observation	

	3) determining if similar nonconformities exist, or could potentially occur?	Yes	Observation	
	c) implement any action needed?	Yes	Observation	
	d) review the effectiveness of any corrective action taken?	Yes	Observation	
	e) make changes to the Information Security Management System, if necessary?	Yes	Observation	
	Are the corrective actions appropriate to the effects of the nonconformities encountered?	Yes	Observation	
	Does the organization retain documented information as evidence of: a) the nature of the nonconformities and any subsequent actions taken; and b) the results of any corrective action?	Yes	Observation	
10.2.	**Continual Improvement**			
	Does the organization continually improve the suitability, adequacy and effectiveness of the Information Security Management System?	Yes	Observation	WWISE is conducting a gap assessment for the first time on behalf of OMS. No non-conformities have been raised prior to the gap assessment.

Clause	Control Objective	ISOIEC 27001:2022 Annex A Clause Questionnaire	Yes/No	NCR / Observation	Comments
5.1	Policies for information security	Do security policies exist? Are all policies approved by management? Are policies properly communicated to employees?	No	Major NCR	OMS has not yet documented the information security policies as required by the requirements of the standard. No communication of current IS policies and approval could be verified at the time of audit.
		Are security policies subject to review? Are the reviews conducted at regular intervals? Are reviews conducted when circumstances change?	No	Major NCR	
5.2	Information security roles and responsibilities	Are responsibilities for the protection of individual assets, and for carrying out specific security processes, clearly identified and defined and communicated to the relevant parties?	No	Major NCR	Responsibilities for carrying out specific security processes have not been clearly identified, defined, and communicated to the relevant parties or appointed ISO champions within the different units or department.

5.3	Segregation of duties	Are duties and areas of responsibility separated, in order to reduce opportunities for unauthorized modification or misuse of information , or service?	Yes	N/A	Duties and areas of responsibility are separated, to reduce opportunities for unauthorised modification or misuse of information, or service. There are daily stand-up meetings that governs the team, and tasks are allocated through the ticketing system on MS teams canal board to everyone and the head of the team is the responsible person to assign to everyone.
5.4	Management responsibilities	Are managers (of all levels) engaged in driving security within the business? Does management behaviour and Policy drive, and encourage, all employees, contractors and 3rd party users to apply security in accordance with established policies and Procedures?	Yes	Minor NCR	There are established policies and procedures in place within OMS; however, they need to be document controlled and reviewed according to the control of documents procedure.
5.5	Contact with authorities	Is there a Procedure documented, when, and by whom contact with relevant authorities (law enforcement etc.) will be made? Is there a process which details how and when contact is required? Is there a process for routine contact and intelligence	No	Minor NCR	There is no documented procedure for contact with relevant authorities (law enforcement etc.).

		sharing?			
5.6	Contact with special interest groups	Do relevant individuals within the organisation maintain active membership in relevant special interest groups?	No	Minor NCR	Individuals within OMS do not maintain active memberships in relevant special interest groups.
5.7	Threat intelligence	Is there a process in place to help mitigate potential attacks and harmful events occurring in cyberspace? Is there a tool that tracks and monitors potential attacks/threats and sends out alerts? Is there a system in place to prevent and protect against potential attacks?	No	Major NCR	There is no process in place to mitigate potential attacks and harmful events.
5.8	Information security in project management	Do all forms go through some sort of information security assessment?	No	Minor NCR	Information security requirements are not specified when new systems are introduced.

		Are information security requirements specified when new systems are introduced? When systems are being enhanced or upgraded, are security requirements specified and addressed?	No	Minor NCR	
5.9	Inventory of information and other associated assets	Is there an inventory of all assets associated with information and information processing facilities? Is the inventory accurate and kept up to date?	N/A	N/A	The list of inventory of all assets associated with information and information processing facilities is hosted by finance and could be verified.
		Do all information assets have a clearly defined owner who is aware of their responsibilities?	N/A	N/A	
5.10	Acceptable use of information and other associated assets	Is there an inventory of all assets associated with information and information processing facilities? Is the inventory accurate and kept up to date?	No	Minor NCR	There is no acceptable use form established for handing out assets to employees.
		Is there a Procedure for handling each information classification? Are users	No	Minor NCR	

		of information assets made aware of this Procedure?			
5.11	Return of assets	Is there a process in place to ensure all employees and external users return the organization's assets on termination of their employment, contract or agreement?	No	Minor NCR	OMS does not have a process defined to control the return of assets upon termination of employment and that process has not been formally documented and communicated.
5.12	Classification of information	Is there a Policy governing, information classification?	No	Major NCR	There is no policy governing information classification.
5.13	Labelling of information	Is there a process by which all information can be appropriately classified?	No	Major NCR	The process of labelling assets and information has not been finalised and communicated within the organisation to ensure consistency throughout OMS.
5.14	Information Transfer	Do organizational policies govern how information is transferred? Are Procedures for how data should be transferred made available to all employees? Are	No	Major NCR	There is no policy in place to govern how information is transferred.

		relevant technical controls in place to prevent non-authorized forms of data transfer?			
		Do contracts with external parties and agreements within the organisation detail requirements for securing business information transfer?	No	Major NCR	
		Do security policies cover the use of information transfer while using electronic messaging systems?	No	Major NCR	
5.15	Access control	Is there a documented access control Policy? Is the Policy based on business requirement? Is the Policy communicated appropriately?	No	Major NCR	
		Are controls in place to ensure users only have access to the network resources they have been specially authorized to use and are required for their duties?	No	Major NCR	There is no role-based access control in place that is documented.

5.16	Identity management	Is there a formal user access registration process in place?	No	Major NCR	There are shared credentials from some of the systems internally such as Umami, Contabo Server, and Domains.co.za.
5.17	Authentication information	is there a formal management process in place to control allocation of secret authentication information?	No	Minor NCR	There is no formal policy defined to implemented MFA.
		Is there a Policy document covering the organizations' practices in how secret authentication information must be handled? Is this communicated to all users?	No	Minor NCR	
		Are password systems interactive? Are complex passwords required?	No	Minor NCR	The organisation has not effectively defined and documented a password policy.
5.18	Access rights	Is there a formal user access provisioning process in place to assign access rights for all user types and services?	No	Major NCR	Access rights are not controlled and reviewed.
		Is there a process for asset owners to review access rights to their assets on a regular	No	Major NCR	

		basis? Is this review process verified?			
		Is there a process to ensure user access rights are removed on termination of employment or contract, or adjusted upon changed of role?	No	Major NCR	
5.19	Information security in supplier relationships	Is information security included in contracts established with supplier and service providers? Is there an organisation-wide risk management approach to supplier relationships?	No	Minor NCR	There is no clause in the supplier contracts that govern or manage how appropriate technical and organisational measures are implemented to ensure the confidentiality, integrity, and availability of client data, including compliance with ISO/IEC 27001 controls.
5.20	Addressing information security within supplier agreements	Are suppliers provided with documented security requirements? Is supplier access to information assets and infrastructure controlled and monitored?	No	Minor NCR	There is no clause in the supplier contracts that govern or manage how appropriate technical and organisational measures are implemented to ensure the confidentiality, integrity, and availability of client data, including compliance with ISO/IEC 27001 controls.
5.21	Managing information security in the ICT supply chain	Do supplier agreements include requirements to address information security within the service and product supply chain?	No	Minor NCR	
5.22	Monitoring ,	Are suppliers subject to	No	Major NCR	There is no documented process in place to review current suppliers.

	review and change management of supplier services	regular review and audit?			
		Are changes to provision of services subject to management process which includes the communication of Policies and Procedures related to Security Controls?	No	Major NCR	
5.23	Information security for use of cloud services	Is there a documented best practice, procedure, and guideline in place to secure cloud environments?	No	Major NCR	All the cloud service providers sourced do not follow a formal onboarding process.
5.24	Information security incident management planning and preparation	Are management responsibilities clearly identified and documented in the incident management processes?	No	Major NCR	There are no incident management processes.
5.25	Assessment and decision on information security events	Is there a process to ensure information security events are properly assessed and classified?	No	Major NCR	There is no process to ensure information security events are properly assessed and classified.
5.26	Response to information security	Is there an incident response process which reflects the classification	No	Major NCR	There is no incident response plan.

	incidents	and severity of information security incidents?			
5.27	Learning from information security incidents	Is there a process or framework which allows the organisation to learn from information security incidents and reduce the impact / probability of future events?	No	Minor NCR	There is no formal process for logging issues/incidents within OMS.
5.28	Collection of evidence	Is there a forensic readiness Policy? In the event of an information security incident is relevant data collected in a manner which allows it to be used as evidence?	No	Minor NCR	There is no system in place that manages the collection of evidence to use as records in an event of an incident.
5.29	Information security during disruption	Is information security included in the organization's continuity plans?	No	Major NCR	The organisation's security function has not been documented, implemented, and maintained.
		Does the organization's security function have documented, implemented and maintained processes to maintain continuity of service during an adverse situation?	No	Major NCR	
		Are continuity plans	No	Major NCR	ICT readiness for business continuity is not planned, implemented,

		validated and verified at regular intervals?			maintained, and tested based on business continuity objectives and ICT continuity requirements.
5.30	ICT readiness for business continuity	Is ICT readiness planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements?	No	Major NCR	
5.31	Legal, statutory, regulatory and contractual requirements	Has the organisation identified and documented all relevant legislative, regulatory, or contractual requirements related to security?	No	Minor NCR	OMS does not have a legal register in place.
		Are cryptographic controls protected in accordance with all relevant agreements, legislation and regulations?	No	Minor NCR	OMS does not have a legal register in place.
5.32	Intellectual property rights	Is compliance documented?	No	Minor NCR	At the time of the GAP we could not verify of OMS has licensed any of their Intellectual property rights including software or document copyright, design rights, trademarks, patents, and source code licences.
5.33	Protection of records	Does the organisation keep record of all intellectual property rights and use of proprietary software products? Does the	No	Minor NCR	OMS keep record of all intellectual property rights and use of proprietary software products. The initiative of managing the records has been established, however not effectively followed throughout the organisation. There is no retention policy that governs how long information should be retained for internally.

		organisation monitor for the use of unlicensed software?			
5.34	Privacy and protection of PII	Are records protected from loss, destruction, falsification and unauthorized access or release in accordance with legislative, regulatory, contractual and business requirements?	Yes	N/A	Records are protected from loss, destruction, falsification, and unauthorised access or release in accordance with legislative, regulatory, contractual, and business requirements.
5.35	Independent review of information security	Is the organizations approach to managing information security subject to regular independent review? Is implementation of security controls subject to regular independent reviews?	No	Minor NCR	OMS has not conducted an independent review of their information security controls as per the standard. People, processes, and technologies are not reviewed independently at planned intervals.
5.36	Conformance with policies, rules and standards for information security	Does the organisation instruct managers to regularly review compliance with policies and Procedures with their area of responsibility? Are records of these reviews	No	Major NCR	OMS has not reviewed compliance with policies and procedures. These records of these reviews are not conducted.

		maintained?			
		Does the organisation regularly conduct technical compliance reviews of its information systems?	No	Major NCR	No pen tests have been conducted thus far in 2025.
5.37	Documented operating procedures	Are operating Procedures well documented? Are the Procedures made available to all users who need them?	Yes	Minor NCR	There are operating Procedures documented; however, they are not document controlled.
6.1	Screening	Are background verification checks carried out on all new candidates for employment? Are these checks approved by management? Are the checks compliant with relevant laws, regulations and ethics? Are the level of checks required support by business risk assessments?	No	Major NCR	Background verification checks for qualifications are done However, there is no tool in place to verify criminal and credit checks for employees.
6.2	Terms and conditions of employment	Are all employees, contractors and third party users asked to sign confidentially and non-	Yes	N/A	All employees, contractors and third-party users asked sign confidentially and non-disclosure agreements.

		disclosure agreements? Do employment/ services contacts specifically covers the need to protect business information?			
6.3	Information security awareness, education and training	Do all employees, contractors and third-party users undergo regular security awareness training appropriate to their role and function within the organisation?	Yes	N/A	Information security awareness has been conducted for employees.
6.4	Disciplinary process	Is there a formal disciplinary process which allows the organisation to take action against employees who have committed an information security breach? Is this communicated to all employees?	Yes	N/A	There is a formal disciplinary process which allows the organisation to take action against employees who have breached internal policies and procedures.

6.5	Responsibilities after termination or change of employment	Is there a documented process for terminating or changing employment duties? Is any information security duties which survive employment communicated to the employee or contractor? Is the organisation able to enforce compliance with any duties that survive employment?	No	Minor NCR	OMS does not have a documented process for terminating or changing employment duties.
6.6	Confidentiality or non-disclosure agreements	Do employees, contractors, and agents sign confidentiality or non-disclosure agreements? Are these agreements subject to regular review? Are records of the agreement maintained?	Yes	N/A	Employees, contractors, and agents sign confidentiality or non-disclosure agreements.
6.7	Remote working	Is there a Policy of teleworking? Does this have management approval? Is there a set of processes for remote workers to get access? Are teleworking given the advice and equipment to protect	Yes	N/A	There is a policy that governs remote working.

		their assets?			
6.8	Information security event reporting	Is there a process for timely reporting of information security events? Is there a process for reviewing and acting on reported information security events?	No	Major NCR	There is no process for reporting of identified information security weakness.
		Is there a process for reporting of identified information security weakness? Is this process widely communicated? Is there a process for reviewing and addressing reports in a timely manner?	No	Major NCR	
7.1	Physical security perimeters	Is there a designated security perimeter? Are sensitive or critical information areas segregated and appropriately controlled?	Yes	N/A	During the time of the audit, we could verify that all the windows with in OMS have security doors, however.
7.2	Physical entry	Do secure areas have suitable entry control systems to ensure only authorized personnel	No	Minor NCR	Entrance area at OMS has suitable entry control systems to ensure only authorised personnel have access. However, there is no access control system at the front reception to manage access within the OMS office.

		have access?			
		Are there separate delivery / loading areas? Is access to these areas controlled? Is access from loading areas isolated from information processing facilities?	No	Minor NCR	Entrance area at OMS have suitable entry control systems to ensure only authorised personnel have access. However, there is no access control system at the front reception to manage access within the OMS office. There is no Visitor logbook to manage access within OMS office.
7.3	Securing offices, rooms and facilities	Have offices, rooms and facilities been designed and configured with security in mind? Do processes for maintaining security (e.g. locking up, clear desks, etc.) exist?	Yes	N/A	Offices, rooms, and facilities been designed and configured with security in mind at OMS. Doors are always closed for security reasons.
7.4	Physical security monitoring	Is there a process in place to monitor the physical security measures used to protect the personnel and property? Is there a security operating centre (SOC)?	No	Minor NCR	There is no process in place to monitor the physical security measures used to protect the personnel and property for OMS.
7.5	Protecting against external and environmental threats	Have physical protection measures to prevent natural disasters, malicious attacks or accidents been designed	Yes	N/A	The server room caters for environmental threats such as flooding as the server cabinet is elevated to shoulder height.

		in?			
7.6	working in secure areas	Do secure areas exist? Where they do exist, do secure areas have suitable policies and processes? Are the policies and processes enforced and monitored?	N/A	N/A	There are no secure areas.
7.7	Clear desk and clear screen	Clear Screen and Clear Desk Policy Implemented?	No	Major NCR	A clear desk and clear desk policy has not been implemented.
7.8	Equipment siting and protection	Are environmental hazards identified and considered when equipment locations are selected? Are the risks from unauthorized access / passer-by considered when siting equipment?	No	Major NCR	Observations revealed lack of maintenance in the server room, characterised by general housekeeping practices, including no cable management, presence of access boxes. Furthermore, assets lack proper labelling which were identified within the rack.
7.9	Security of assets off-perimeters	Is there a Policy covering security assets off-site? Is this Policy widely communicated?	No	Minor NCR	There is no policy covering security assets off-site.

7.10	Storage media	Is there a Policy governing removable media? Is there a process covering how removable media is managed? Are the Policy and processes (es) communicated to all employees using removable media?	No	Minor NCR	There is no policy that governs removable media.
		is there a formal Procedure governing how removable media is disposed?	No	Minor NCR	There is no policy that governs removable media.
		Is there a documented Policy and process detailing how physical media should be transported? Is media in transport protected against unauthorized access, misuse or corruption?	No	Minor NCR	There is no policy that governs removable media.
		Is there a process monitoring how assets are removed from site? Is the process enforced? Are spot checks carried out?	No	Minor NCR	There is no policy that governs removable media.
7.11	Supporting utilities	Is there a Ups system or back up generator? Have these been tested	No	Minor NCR	There is no UPS onsite for the cabinet. The generator onsite belongs to the building management.

		within an appropriate timescale?			
7.12	Cabling security	Have risk assessments been conducted over the location of power and telecommunications cables? Are they located to protect from interference, interception or damages?	No	Minor NCR	There is a cabinet housing critical data/network infrastructure of the organization, however the cables are not labelled to specify which cables are the Uplink (Lan) or WAN link from the ONT.
7.13	Equipment maintenance	Is there a rigorous equipment maintenance schedule?	No	Major NCR	There is no maintenance schedule for OMS.
7.14	Secure disposal or re-use of equipment	I there a Policy covering how information assets may be reused? Where data is wiped, is this properly verified before reuse / disposal?	No	Minor NCR	There is no policy covering how information assets may be reused.
8.1	User end point devices	Does a mobile device Policy exist? Does the Policy have management approval? Does the Policy document and address additional risks from using mobile devices (e.g. theft of asset, use of open wireless hotspots etc.)?	No	Minor NCR	There is no documented policy that governs unattended user, equipment ensuring their devices are locked whilst not being present at their workstations.

		Unattended user, equipment, does the company have a culture in ensuring their devices are locked whilst not being present at their workstations?	No	Minor NCR	
8.2	Privileged access rights	Are privileged access accounts separately managed and controlled?	No	Minor NCR	Privileged access accounts are not separately managed and controlled.
8.3	Information access restriction	Is access to information and application system function restricted in line with access control Policy?	No	Major NCR	There is no access control policy or reviews inhouse that has been conducted manage which users have access to certain systems.
8.4	Access to source code	Are Read and write access to source code, development tools and software libraries appropriately managed?	Yes	N/A	everyone who is a dev has access to the source code. It is controlled between accounts by separating accounts and managing access/read/write.
8.5	Secure authentication	Where the access control Policy requires it, is access controlled by a secure log-on Procedure?	Yes	Minor NCR	OMS makes use of MFA on some of their internal System. In systems that are using a shared account there Is no MFA configured.
8.6	Capacity management	Is there a capacity management process in place?	Yes	Minor NCR	There is a system called Beszel that handles capacity management, monitors containers and servers for OBSE production. Thresholds for capacity alerts for CPU and average load are not documented and configured to be triggered by excessive use of CPU usage, Memory and disk usage.

8.7	Protection against malware	Are processes to detect malware in place? Are processes to prevent malware spreading in place? Does the organisation have a process and capacity to recover from a malware infection?	Yes	N/A	OMS uses ESET Anti-Virus 18.1 to manage and monitor inhouse technical vulnerability.
8.8	Management of technical vulnerabilities	Does the organisation maintain updated and timely information on technical vulnerabilities? Is there a process to risk assess and react to any new vulnerabilities as they are discovered?	No	Major NCR	OMS does not maintain updated information on technical vulnerabilities and there is no process to risk assess and react to any new vulnerabilities as they are discovered
		Does the organisation regularly conduct technical compliance reviews of its information systems?	No	Major NCR	OMS does not maintain updated information on technical vulnerabilities and there is no process to risk assess and react to any new vulnerabilities as they are discovered
8.9	Configuration management	Is there a process in place to manage and control configurations of the information system to enable security and facilitate risk management?	No	Minor NCR	Version control is managed through GitHub. There is a process in place; however, it is not documented.

8.10	Information deletion	Is there a process in place to prevent permanent data loss? Is there a process in place that governs the backup of data before deletion?	No	Minor NCR	Information deletion is addressed as and when it comes. User machines are wiped before they are handed over to the next employee. There is no official method of disposing of information on old assets that are not being utilised by employees.
8.11	Data masking	Is there a process of modifying sensitive data (hiding/masking sensitive information) in such a way that it is of no or little value to unauthorized intruders while still being usable by software or authorized personnel?	No	Major NCR	**Pseudonymisation** (*Replacing identifying fields in a dataset with artificial identifiers or pseudonyms (e.g., replacing a name with a user ID or code*), **anonymisation** (transforming personal data so that individuals cannot be identified), **salting techniques (Adding a random value (salt) to data before hashing it to make the result unique)** have not been standardised and deployed.
8.12	Data leakage prevention	Is there a system in place to prevent data leakage? Can all data be protected when not connected to the corporate network? In an event of a data leakage, is there a documented plan in place to mitigate the data breach/leakage?	No	Major NCR	Data Leakage Prevention requirements of ISO/IEC 27002:2022 have not been defined and implemented.
8.13	Information backup	Is there an agreed backup Policy? Does the organization's backup Policy comply with relevant legal	Yes	Minor NCR	There is a repository outside of Github called Gitea - this server is mirroring the application. Coolify backups to slef hosted serer.(1 server is hosted is in Germany) and another is USA (Newak). Other backups are running from user SharePoint and one drive. However, there is no documented backup policy.

		frameworks? Are backups made in accordance with the Policy? Are backups tested?			
8.14	Redundancy of information processing facilities	Do information processes facilities have sufficient redundancy to meet the organizations availability requirements?	Yes	N/A	From the production environment, there servers that are replicating the core environment that is sitting on GitHub.
8.15	Logging	Are appropriate event logs maintained and regularly reviewed?	No	Minor NCR	There is no tool to manage system logs and protect the logs from system users.
		Are logging facilities protected against tampering and unauthorized access?	No	Minor NCR	There is no tool to manage system logs and protect the logs from system users.
		Are sysadmin / sysop logs maintained, protected and regularly reviewed?	No	Minor NCR	There is no tool to manage system logs and protect the logs from system users.
8.16	Monitoring activities	Is there a process in place to monitor activities?	No	Minor NCR	There are no formal monitoring methods that have been conducted to monitor anomalous behaviour in the OMS's Infrastructure.
8.17	Clock synchronization	Are all clocks within the organisation synchronised?	No	Minor NCR	There is no NTP (Network Time Protocol) server that endpoints and devices on the domain and Network synchronise to.
8.18	Use of privileged utility programs	Are privilege utility programs restricted and monitored?	Yes	Minor NCR	Access to privileged utility programmes is not restricted and monitored with the use of Active Directory.

8.19	Installation of software on operational systems	Is there a process in place to control the installation of software onto operational systems?	No	Minor NCR	There is no process in place to control the installation of software onto operational systems.
		Are there controls in place to restrict how users install software?	No	Minor NCR	There is no process in place to control the installation of software onto operational systems.
8.20	Networks security	Is there a network management process in place?	No	Major NCR	There is no network management process in place.
8.21	Security of network services	Does the organisation implement a risk management approach which identifies all network services and service agreements? Is security mandated in agreements and contracts with service providers (in house and outsourced)? Are security related SLAs mandated?	No	Minor NCR	Presently, there are no authentication controls in place for accessing administrative network controls within the organisation. Moreover, the system logs (sys logs) and event logs are not currently reviewed or monitored within the organization.
8.22	Segregation of networks	Does the network topology enforce segregation of networks for different tasks?	Yes	Minor NCR	There are 3 different networks configured internally, however the usage of it is not enforced to manage guests and internal staff members
8.23	Web filtering	Is there a web filtering tool? If so, is it regularly monitored and reviewed? Is there a	No	Major NCR	Websites such as uTorrent, adult content, and gambling sites can be accessed. Malicious software can be downloaded on the LAN and WAN.

		policy in place that monitors the mitigation process for web filtering alerts and incidents received?			
8.24	Use of cryptography	Is there a Policy on the use of cryptographic controls?	No	Major NCR	There is no encryption method that is utilized internally such as BitLocker.
		Is there a Policy governing the whole lifecycle of cryptographic keys?	No	Major NCR	There is no documented policy to align ISO/IEC 27002:2022 standard.
8.25	Secure development life cycle	Does the organisation develop software or systems? If so, are there policies mandating the implementation and assessment of security controls?	Yes	N/A	During the time of the audit, the policies mandating the implementation and assessment of security controls could not be verified.
8.26	Application security requirements	Do applications which send information over public networks appropriately protect information against fraudulent activity, contract dispute, unauthorized modification?	Yes	N/A	The application that is developed in-house does not store any confidential data in its database; it just executes a processing mechanism of data and users can then extract at their own accord. However, the system does not transmit, misroute any of the confidential data.

		Are controls in place to prevent incomplete transmission, misrouting, unauthorized disclosure, unauthorized message duplication or replay attacks?	Yes	N/A	The application that is developed in-house does not store any confidential data in its database, it just executes a processing mechanism of data and users can then extract at their own accord. However, the system does not transmit, misroute any of the confidential data.
8.27	Secure system architecture and engineering principles	Does the organisation have documented principles on how systems must be engineered to ensure security?	No	Minor NCR	There are no documented principles on how systems must be engineered to ensure security.
8.28	Secure coding	Is there a regular expression/database query to process input data? Authentication - Does the code check that the request really is coming from the person or system it claims to be coming from? Authorization - Does the code check the user is allowed to perform the action in question? Accounting - Does the code record who did what, so that you can check back later in case there is an issue?	Yes	N/A	When the code is deployed to GitHub, users have their own accounts to deploy, and it managed through the head of IT. The system keeps track of changes and deployments.

8.29	Security testing in development and acceptance	Where systems or applications are developed are they tested as part of the development process?	Yes	N/A	Systems and applications that are developed are tested as part of the development process.
		Is there an established process to accept new systems/ applications or upgrades, into production use?	No	Minor NCR	There is no process to accept new systems/applications or upgrades, into production use.
8.30	Outsourced development	Where development has been outsourced is this supervised? Is externally developed code subject to a security review before deployment?	Yes	N/A	No.
8.31	Separation of development, test and production environments	Does the organisation enforce segregation of development, test and operational environment?	Yes	N/A	The organisation enforces segregation of development, test, and operational environment.
		has a secure development environment been established? Do all projects utilize the secure environment appropriately during the system development lifecycle?	Yes	N/A	The organisation enforces segregation of development, test, and operational environment.
8.32	Change management	Is there a controlled change management	No	Minor NCR	There is no change control procedure and process are in placed at OMS.

		process in place?			
		Is there a formal change control process for software development?	No	Minor NCR	There is no formal change control process for software development.
		Is there a process to ensure a technical review is carried out when operating platforms are changed?	No	Minor NCR	There is no process to ensure a technical review is carried out when operating platforms are changed.
		Is there a Policy in place which mandates when and how software packages can be changed or modified?	No	Minor NCR	There is no Policy in place which mandates when and how software packages can be changed or modified.
8.33	Test information	Is there a process for selecting test data? Is test data suitably protected?	Yes	N/A	The organisation enforces segregation of development, test, and operational environment.
8.34	Protection of information systems during audit testing	Are IS systems subject to audits? Does the audit ensure business disruption is minimized?	No	Minor NCR	There has not been an IS systems audit recently.

CONCLUSION

In conclusion, Owethu Managed Services has been maintaining various controls per the ISO/IEC 27001:2022 standard. The results of the gap assessment conducted are detailed below:

52 SYSTEM GAPS

34 PROCESS GAPS

0 OPPORTUNITIES/ RECOMMENDATIONS FOR IMPROVEMENT

While some documentation and controls have been implemented and are maintained, a number of areas have been identified as non-conforming to the standard. A total of 52 System GAPS, 34 Process GAPS and 0 opportunities for improvement were identified as per the ISO/IEC 27001:2022 standard. If Owethu Managed Services corrects all the System GAPS and Process GAPS, they will adhere to all the relevant requirements of the ISO/IEC 27001:2022 standard.

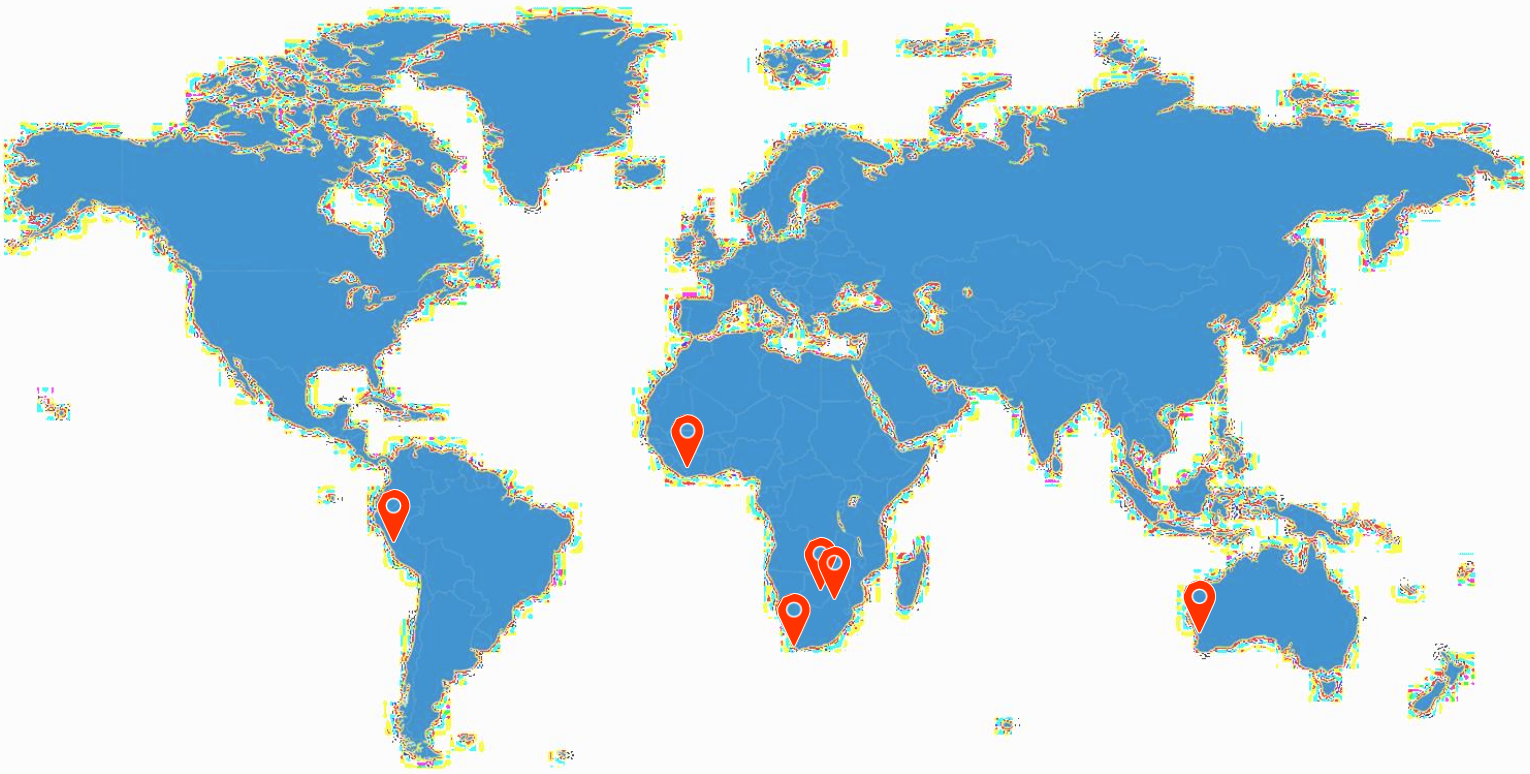
Acknowledgement,

Lead Implementers of ISO Management Systems

Muhammad Ali
Managing director
Masters & Honours (M.Sc./BSc) Industrial and Systems Engineering:
UP B-Tech in Industrial and Systems Engineering T.U.T.:
PhD Candidate of UP
Registered Lead Implementer and Auditor on 10 different ISO Standards

+27 861 099 473 (WWISE)
+27 72 300 5065
m.ali@wwise.co.za
www.wwise.co.za
254 Hall Street, Westend Office Park
Building 2 Second floor, Die Hoewes,
Centurion, 0157 South Africa

CONTACT US



PRETORIA, CENTURION HEAD OFFICE

254 Hall Street, Westend Office Park,
Building 2, Floor 2
+27 (86) 109-9473
+27 (12) 644-0142
admin@wwise.co.za

CAPE TOWN, CENTURY CITY OFFICE

Unit 127, The Quays, 4 Park Lane,
Century City
+27 (21) 525-9159
admin@wwise.co.za

We will be opening branches in Perth: Australia, Accra: Ghana, and Gaborone: Botswana