ISO 27001 AUDIT CHECKLIST

ISO 27001 Checklist	Fully Implemented	Partially Implemented	Yet to Start
Have you established behavioral standards which are defined in the Code of Business Conduct and made it available to all staff members on the company intranet?	☐	☐	☐
Do you maintain an Organizational Structure to define authorities, facilitate information flow and establish responsibilities?	☐	☐	☐
Have you clearly defined job responsibilities for client serving, IT and engineering positions (via OKRs, Job Descriptions etc.) to increase the operational effectiveness of the organisation?	☐	☐	☐
Are your new hires evaluated for competence in their expected job responsibilities?	☐	☐	☐
Do all your new hires undergo a background check as part of their onboarding process?	☐	☐	☐
Do all your new staff review and acknowledge company policies as part of their onboarding?	☐	☐	☐
Have you established an Information Security Awareness training, and made its content available for all staff on the company intranet?	☐	☐	☐
Do all your staff complete Information Security Awareness training upon hire, and undergo Information Security Awareness training annually?	☐	☐	☐
Do you periodically review the job responsibilities of all employees in client serving, IT, Engineering and Information Security roles?	☐	☐	☐
Do your new staff review and acknowledge the Code of Business Conduct upon hire, and that all staff members review and acknowledge it annually?	☐	☐	☐
Do all your staff review and acknowledge company policies annually?	☐	☐	☐
Are your policies and procedures available to all staff members via the company intranet?	☐	☐	☐
Do you display the most current information about your services on the company website? (which is accessible to its customers)	☐	☐	☐
Have you clearly provided information to employees, via the Information Security Policy, on how to report failures, incidents, concerns, or other complaints related to the services or systems in case of any untoward event?	☐	☐	☐
Have you provided information to your customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided in the event there are problems?	☐	☐	☐

ISO 27001 AUDIT CHECKLIST

ISO 27001 Checklist	Fully Implemented	Partially Implemented	Yet to Start
Do you have a formally documented policies and procedures to govern risk management?	☐	☐	☐
Do you perform a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair your systems' security commitments and requirements?	☐	☐	☐
Have you assessed each risk and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of your ISMS? Are all the risks mapped to mitigating factors that address some or all of the risk?	☐	☐	☐
Have you considered the potential for fraud when assessing risks? This is an entry in the risk matrix.	☐	☐	☐
Do you perform a formal vendor risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify vendors that are critical to your systems' security commitments and requirements?	☐	☐	☐
Has your Senior Management assigned the role of Information Security Officer, who will delegate the responsibility of planning, assessing, implementing and reviewing the internal control environment?	☐	☐	☐
Does your senior management review and approve all company policies annually?	☐	☐	☐
Does your senior management review and approve the state of the Information Security program annually?	☐	☐	☐
Does your senior management review and approve the Organizational Chart for all employees annually?	☐	☐	☐
Does your senior management review and approvesthe "Risk Assessment Report" annually?	☐	☐	☐
Does your senior management review and approvesthe list of people with access to production console annually?	☐	☐	☐
Does your senior management review and approve the "Vendor Risk Assessment Report" annually?	☐	☐	☐
Does your senior management review and evaluate all subservice organizations periodically, to ensure that the commitments to your customers can be met?	☐	☐	☐
Has your organization a developed a set of policies that establish expected behavior with regard to the Company’s control environment?	☐	☐	☐

ISO 27001 AUDIT CHECKLIST

ISO 27001 Checklist	Fully Implemented	Partially Implemented	Yet to Start
Does your organization provide guidance on decomissioning of information assets that contain classified information in the Media disposal policy?	☐	☐	☐
Are all your production database[s] that store customer data are encrypted at rest?	☐	☐	☐
Is your production host protected by a firewall with a deny-by-default rule? Deny by default rule set is a default on your cloud provider.	☐	☐	☐
Is user access to your application secured using https (TLS algorithm) and industry standard encryption?	☐	☐	☐
Do you maintain a list of production infrastructure assets and segregate production assets from its staging/development assets?	☐	☐	☐
Have you established an Incident Management & Response Policy, which includes guidelines and procedures to be undertaken in response to information security incidents? This is available to all staff members via the company intranet.	☐	☐	☐
Do you maintain a record of information security incidents?	☐	☐	☐
Do you identify vulnerabilities on your company's platform through the execution of regular vulnerability scans?	☐	☐	☐
Do you track all vulnerabilities, and resolves them as per the Vulnerability Management Policy?	☐	☐	☐
Have you documented Business Continuity & Disaster Recovery Policies,that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident?	☐	☐	☐
Do you have a documented Data Backup Policy that's available for all staff on the company intranet?	☐	☐	☐
Do you back-up your production databases periodically?	☐	☐	☐
Are your data backups restored and tested annually?	☐	☐	☐
Is you infrastructure configured to generate audit events for actions of interest related to security which are reviewed and analyzed for anomalous or suspicious activity?	☐	☐	☐
Are your production assets continuously monitored to generate alerts and take immediate action where necessary?	☐	☐	☐

ISO 27001 AUDIT CHECKLIST

ISO 27001 Checklist	Fully Implemented	Partially Implemented	Yet to Start
Do you identify vulnerabilities on the company platform through annual penetration testing exercise conducted by a qualified third-party service provider?	☐	☐	☐
Do you have a documented Change Management Policy that's available to all Staff Members via the company intranet?	☐	☐	☐
Do you use a change management system to track, review and log all changes to the application code?	☐	☐	☐
Is your change management system is configured to enforce peer reviews for all planned changes? For all code changes, the reviewer must be different from the author.	☐	☐	☐
Do you have a documented Risk Assessment and Management Policy that describes the processes in place to identify risks to business objectives and how those risks are assessed and mitigated?	☐	☐	☐
Do you have a documented Vendor Management Policy that provides guidance to staff on performing risk assessment of third-party vendors?	☐	☐	☐
Do you have a documented Confidentiality Policy that's available for all staff on the company intranet?	☐	☐	☐
Have you implemented physical and/or logical labelling of information according to the documented Data Classification Policy?	☐	☐	☐
Do you have a documented Data Retention Policy that's available for all staff on the company intranet?	☐	☐	☐
Do you periodically test the Disaster Recovery Plan and document your learnings?	☐	☐	☐
Do the customer data used in non-production environments require the same level of protection as the production environment?	☐	☐	☐
Do your Board of Directors meet periodically to provide independent oversight on the functioning of the organization?	☐	☐	☐
Do you have a documented Endpoint Security Policy that's available for all staff on the company intranet?	☐	☐	☐
Do you have a documented Acceptable Usage Policy that's made available for all staff on the company intranet?	☐	☐	☐
Do you have a documented Encryption Policy that'smade available for all staff on the company intranet?	☐	☐	☐

ISO 27001 AUDIT CHECKLIST

ISO 27001 Checklist	Fully Implemented	Partially Implemented	Yet to Start
Do you have a documented Password Policy that's made available to all staff members on the company intranet?	☐	☐	☐
Are all your critical endpoints encrypted to protect them from unauthorised access?	☐	☐	☐
Have you appointed an owner of infrastructure, who is responsible for all assets in the inventory?	☐	☐	☐
Do you have continuous monitoring system, to track and report the health of your information security program to the Information Security Officer and other stakeholders?	☐	☐	☐
Do you have a continuous monitoring system,to alert the security team to update the access levels of team members whose roles have changed?	☐	☐	☐