A reassuringly dull description*

*Reassuringly dull cyber security

ISO:27001 – Ongoing ISMS Management Service

Maintaining a 27001 compliant management system

To maintain an ISO27001 compliant Information Security Management System (ISMS) organisations must demonstrate that they are:

- Maintaining sight of, and continually reassessing, their information security risks
- Reviewing documentation and security controls to ensure they remain relevant
- Ensuring information security objectives are fulfilled and new objectives set as required
- Running an internal audit programme and resolving any findings
- Keeping senior leadership informed about the progress of the ISMS
- Continually improving the ISMS

Generally, your organisation will be required to demonstrate that the *Plan*, *Do*, *Check*, *Act* cycle is continuously functioning, and the ISMS remains relevant. When the need to do this is combined with other issues that can affect a business such as change, incidents, or new opportunities, the maintenance of an ISMS can become complex and time consuming, especially for a small-to-medium sized enterprise.

If you are using **norm**'s recommended online ISMS management platform, **norm.** can help reduce the workload associated with the maintenance of your ISMS. To this end, **norm.** has developed a selection of Service Modules for you to choose from allowing you to utilise our expertise as much or as little as you require.

How does it work?

When you have decided upon the service modules that you need and once your order is received, a member of our Customer Experience team will take ownership of your order and contact you to introduce themselves as your project lead. They will arrange a Welcome call with you to guide you through the process and introduce you to your named **norm.** ISO27001 consultant who will be assigned to assist you.

To derive the maximum benefit from this service your organisation will need to use **norm**'s recommended online ISMS management platform, to provide our Information Security consultants with easy access to your environment and be able to efficiently collaborate with you and your team to ensure the process has the minimum impact on your day-to-day business activities.

If you do not wish to transition to the ISMS.online platform, **norm**. Is willing to discuss alternative service options. Regardless of the platform used, support with your internal audit program will always be available to you.

Risk Management

As a part of maintaining your ISMS, your organisation will need to maintain your information security risk register. To do this you will need to ensure that you are up to date on the current threat landscape, the current state of your organisation and constantly reviewing your risks with those factors in mind.

In order to relieve the effort required by your staff to perfom this activity on an ongoing basis, **Norm**'s Information Security consultants will;

- Provide you with monthly threat reporting, ensuring you stay up to date with current issues and events
- Liaise with your asset owners to review your risks in detail and ensure any treatments/controls are still relevant and working
- Host any risk management meetings with your internal risk managers/committee
- Support the implementation of risk treatments

Internal Auditing

Your organisation will be required to plan and conduct an internal audit programme to assure compliance to the ISMS within your organisation, as well as to review working practices more generally. The standard requires this audit cycle be conducted over a minimum of a 3 year period. However, to get value from your audit programme large portions of the ISMS should be reviewed yearly. To aid you with this **norm.** will;

- Plan an internal schedule or use your own
- Review your documentation
- Hold audit sessions/interviews with key stakeholders to evidence compliance
- Produce internal audit reports
- Provide advice on the remediation of audit findings

Management Reviews

To maintain an effective ISMS, it is imperative that senior leadership remains informed with regard to the performance and effectiveness of the ISMS, allowing them to make effective decisions. This aspect of the service becomes more effective if norm. Is engaged to fully manage the ISMS on your behalf. To aid management reviews **norm.** will;

- Create management review materials ahead of the review meetings every quarter
- Host management review meetings every quarter
- Create and Host Annual management review meetings
- Ensure changes to the ISMS are communicated to all staff and that annual awareness training material is produced and/or delivered

Other Support

In order to aid the delivery of other offerings **norm.** can assist with the operations of other processes and provide additional support, this includes:

- The monitoring of ISMS objectives, to be reported to management
- The monitoring of Non-Conformities and ISMS actions
- Advice and help with the completion of ISMS actions, this may incur extra cost depending on the complexity of those actions
- Advice on decisions and objectives regarding the ISMS

A reassuringly dull description*

*Reassuringly dull cyber security

Service Availability

The **norm.** Information Security consultants and Customer Experience teams are available during UK business hours, Monday to Friday 9:00 to 17:30, excluding public holidays.

Appendix – How do norm's other services support the ISMS?

Norm has a variety of other services that support the Annex A controls of the ISO27001 standard and can be implemented as part of an ISMS implementation, if these controls are not already deployed. These service modules are summarised in the table below:

Service	Service module	ISO27001 Controls
smartbloc.™	Cyber Safety and Awareness Training	A6.3 Information security awareness, education and Training
	Threat Detection and Response (Endpoint)	A8.7 Protection against malware
	Threat Detection and Response	A5.24 – A5.28 Incident Management A5.29 Information security during disruption A6.8 Information Security event reporting A8.15 – A8.16 Logging and Monitoring
	Vulnerability Management and Patch Management	A8.8 Management of Technical Vulnerabilities
	Penetration Testing	A8.8 Management of Technical Vulnerabilities A5.35 Independent review of information security
	smartbloc. [LIVE]	Clause 9.1 Performance Evaluation
Data Protection as a service (DPaaS)	Essentials, Essentials PLUS and Premium	A5.34 Privacy and Protection of Personally Identifiable Information