



GDPR Documentation references

The documents in this toolkit have been designed and created to ensure that you have the most comprehensive set of policies and procedures for your GDPR compliance program.

Documents specifically addressing the unique requirements of the GDPR use the following prefix:

- GDPR (DOC/REC) 0.1

Documents relating to control areas of the GDPR standard have been developed from ISO 27001:2013 Annex A so that you benefit from international best-practice controls; they use the following prefix:

- GDPR-C (DOC/REC) 6.1.3

The numerical identifier for GDPR specific documentation is as follows:

- Guidance documents: 0.1, 0.2, 0.3 and so on
- Policy - Tier 1 document types: 1.0, 1.1, 1.2 and so on
- Procedure – Tier 2 document types: 2.0, 2.1, 2.3 and so on
- Records – Tier 4 document types: 4.0, 4.1, 4.2 and so on

The numerical identifier for management system standard documents relates to the clause requirement from within the standard(s):

- BS 10012:2017 / ISO 27001:2013.

For example, GDPR DOC 7.2 addresses clause 7.2 of BS 10012:2017 & ISO 27001:2013.

This allows your ISMS program to easily integrate and expand GDPR compliance standards with the international information security standard, ISO 27001.

Other Policy & Procedure Document Requirements

The ISMS program will be further expanded to cover your specific requirements from other regulatory bodies, such as Quality in Optometry, Enhanced Services, etc.

The ISMS program has been developed so that it can integrate with an information security management system (for example, the IG Toolkit for QIO) enabling you to further secure activities with minimal document duplication and efforts.

With the ISMS program, you will be able to easily expand your management system, whether it's information security, environmental, health and safety or quality management systems.

Your ISMS program combines all business components into one coherent system, streamlining process management and operations, meeting business objectives and providing you with:

- A common approach with which to compare risks within different departments.
- Regulation management applicable to your organisational and departmental needs.
- Necessary training, support and awareness programmes typical of the needs of employees and departments.

These benefit your organisation by:

- Saving costs, time and resources
- Avoiding duplication
- Reducing overall risks
- Exposing conflicting objectives
- Focusing on achieving objectives