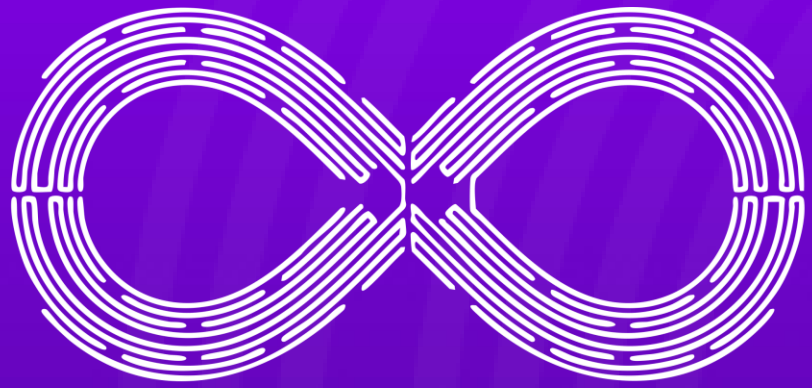
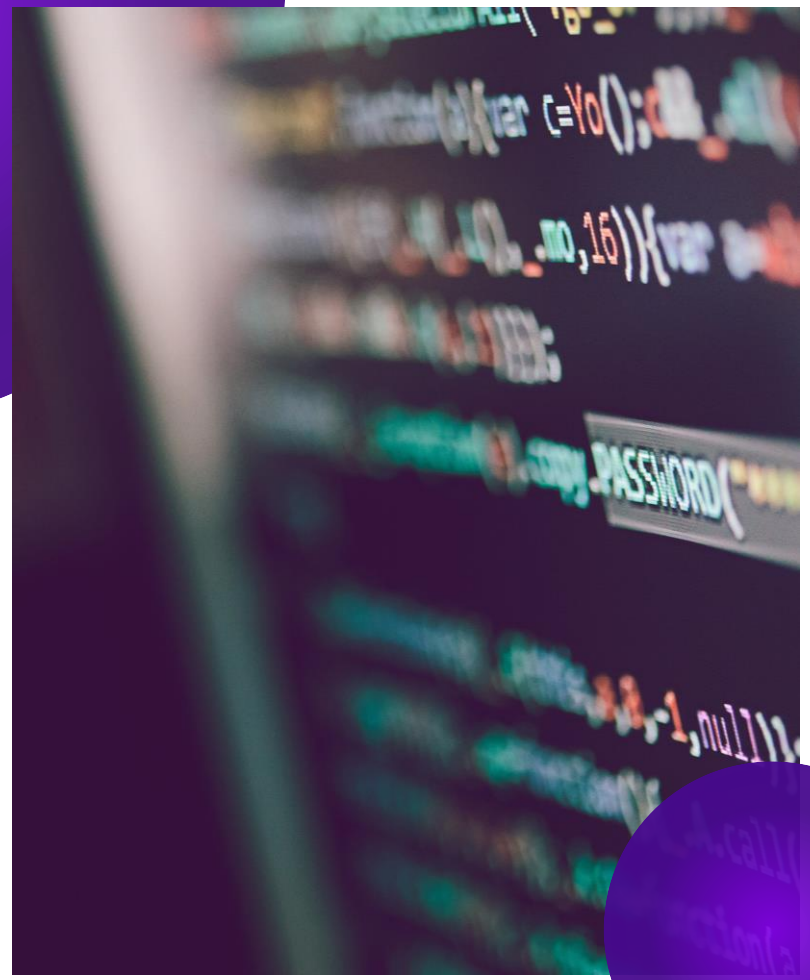


CLEAR LOOP SECURITY

ISO 27001 Project Outline

v1.7 | Classification: Commercial-in-Confidence



Introduction

This document states Clear Loop Security's general approach to ISO 27001 implementation projects, which may be subject to customisation depending on the maturity of the organisation seeking certification.

CLEAR LOOP SECURITY

Overview

Clear Loop Security's approach for ISO 27001 implementation projects is according to the process stated below, with activity split into three phases:

1

PHASE 1

- Asset identification
- Gap analysis
- Risk assessment
- Roadmap creation

2

PHASE 2

- Establish the information security management system (ISMS)
- Develop policies and procedures
- Implement controls

3

PHASE 3

- Perform certification readiness
- Engage external auditor for Stage 1 and Stage 2 audits
- ISO 27001 certification awarded

Phase 1

Phase 1 focuses on identifying the current status of the organisation and determining actions that need to take place for ISO 27001 certification to be successful, Phase 2 provides implementation assistance, and Phase 3 ensures that the organisation is prepared for the external audits and award of ISO 27001 certification.

The effort for Phase 1 is standard, as the same approach is followed for all organisations, so the investment required is easily understood. The amount of assistance each organisation requires in Phases 2 and 3 will differ, depending on the findings from Phase 1, what resources are available to the organisation, and other company-specific factors. Due to this, Phases 2 and 3 tend to be addressed by means of a call-off contract, where we only bill for days that are used, as requested by the client.

Following completion of Phase 1 we will provide a further proposal for Phases 2 and 3.

The overview investment for Phase 1 is:

- Phase 1a (asset discovery) = 5 days
- Phase 1b (gap analysis) = 5 days
- Phase 1c (risk assessment and roadmap) = 3 days
- Phase 1d (workshop) = 2 days
- Phase 1e (ISMS) = 2 days

Total = 17 days

Phase 1 Activities

The initial phase of the project is broken down into distinct steps that are described in detail below. Clear Loop's approach is to ensure that the output of all activities produces mandatory documentation required by ISO 27001 so that the client organisation has already made good progress towards certification.

Phase 1a INFORMATION ASSET DISCOVERY & BUSINESS IMPACT ASSESSMENT

This step will identify the organisation's information assets, which are the critical items which must be protected from loss, tampering or leaks. This will involve interviews with individuals across different departments, usually personnel from HR, operations, IT, admin, finance, senior management, system managers and any other information asset owners. The interviews will be spread across two days, conducted remotely.

The interviews usually commence with a brief overview of the process and then a summary from the interviewee of their job role. Subsequently, we will discuss any information assets that they are aware of, with particular focus on the following:

- Nature of the asset
- Location(s) of the asset
- Impact of a breach of the asset's confidentiality, integrity, and availability
- Legal, reputational, operational, and financial impact of a breach
- The ability and cost of rebuilding the information
- Particular threats to the asset

We will provide guidelines on identifying information assets to the interviewees before these sessions so that they can review the different information assets used in their area of the organisation.

Output

A comprehensive register of all information assets, with ratings for confidentiality, integrity, and availability, in terms of the impact to the organisation should one of these aspects of each asset be breached.

Duration

2 days of interviews and 3 days of reporting. Total of 5 days.

Phase 1b

GAP ANALYSIS AGAINST CONTROLS & MANAGEMENT CLAUSES

This phase will assess the extent to which the organisation has implemented the security controls as stated in ISO 27001/2. As it is assumed that the organisation will not have previously considered the mandatory information security management system (ISMS) clauses from ISO 27001, the primary focus will be on the control catalogue in Annex A (and expanded on in ISO 27002).

This will take the same amount of time as Phase 1a, and the days will be structured in the same way. We will meet with the project sponsor and a senior stakeholder for an initial business discovery and risk appetite meeting at the start of the first day, and also schedule a wrap up session at the close of the second day. Each of the interviews should take no more than one hour, except for the IT interview, which usually takes 2 - 3 hours. As such, we recommend splitting the IT section into two sessions. To make sure that there is sufficient time to review the evidence and consolidate notes, a half hour gap between each meeting is required. There will also be the need throughout the days to review documentation, as discovered during the assessment.

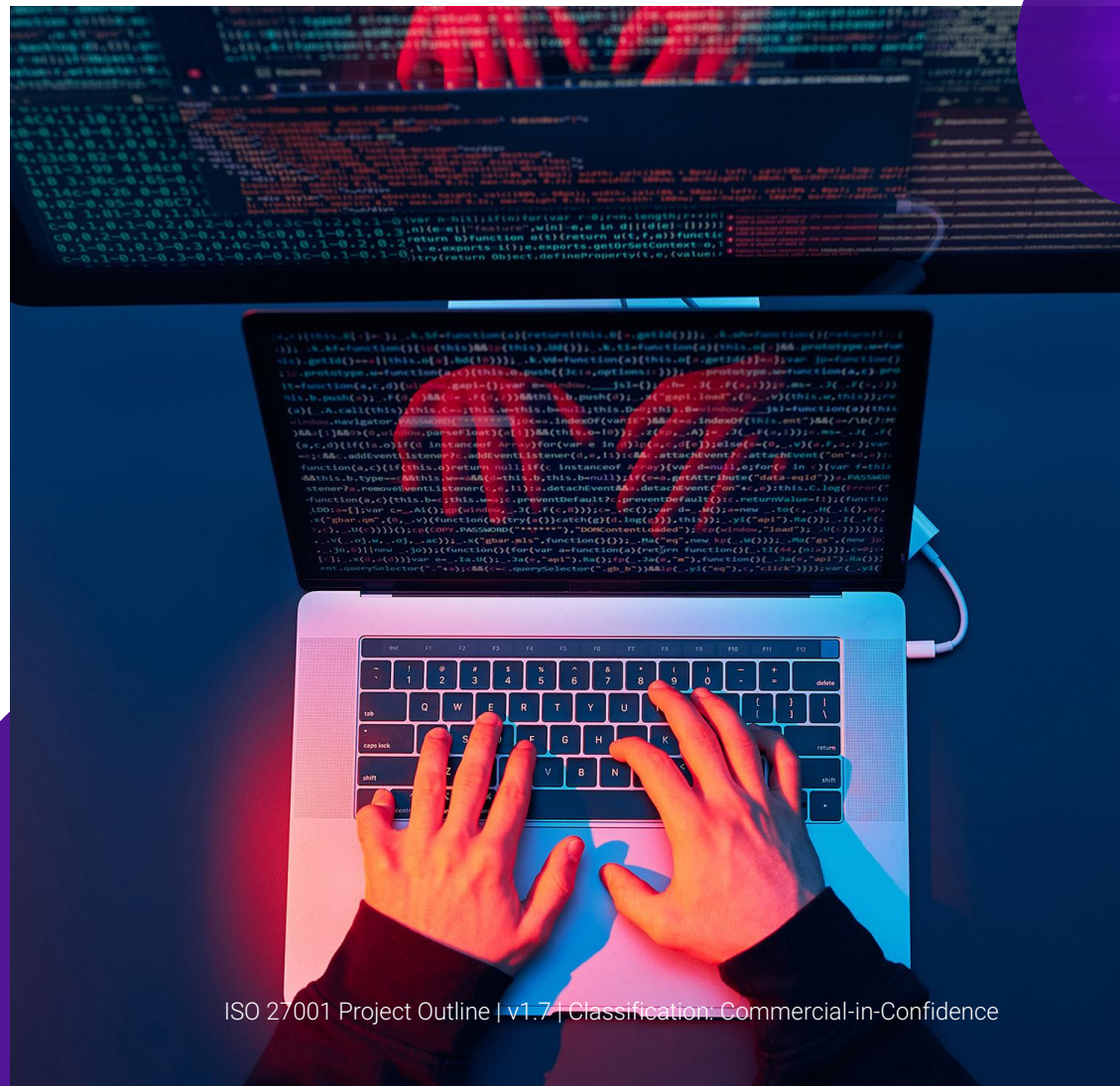
The client should provide access to (or copies of) any existing documentation ahead of time if possible, and also facilitate a walkthrough of each site, including any restricted areas.

Output

- Statement of Applicability showing the extent to which controls are in place, with a maturity rating for each control, and highlighting where work is required to meet the control aims; existing good practice will also be highlighted
- Internal audit report
- Non-conformance register

Duration

2 days of interviews and 3 days of reporting. Total of 5 days.



Phase 1c

RISK ASSESSMENT & ROADMAP CREATION

Building on the information obtained through the previous two phases, we will create a risk assessment that will include:

- Threat assessment, to determine threat actors that would be motivated to have an interest in the organisation and its information assets
- Application of a risk/threat tree to the information assets to determine risks on a graded scale, taking into account existing or missing controls, and stating the impact and likelihood of each risk that could be realised
- Likelihood is based on historic events, events in the sector, and attractiveness of the organisation as a target to the threat actors identified

This risk assessment will show where there are risks above the risk appetite, and which should be addressed as a priority. From this, an ISO 27001 roadmap will be created, to act as a project plan for the implementation of controls and the ISMS. The risk assessment will also provide input to the monitoring and measurement regime that will be key to providing evidence that the ISMS is operating effectively. The risk assessment and roadmap will be created remotely, with no on site days required.

Output

Risk register and implementation roadmap.

Duration

2 days for the risk assessment, 1 day for the roadmap. Total of 3 days.

Phase 1d

WORKSHOP

Once all the deliverables from the previous phases have been provided to the client, a workshop session will be arranged to agree the findings and the roadmap. This will allow the consultant to answer any questions and provide clarifications, and the client to provide input on the practicality of the recommendations and any potential stumbling blocks to implementation. Following the workshop, any required edits to the deliverables will be made and these will be submitted to the client for final sign off.

Output

Updated deliverables.

Duration

1 day for workshop preparation and attendance, 1 day for finalising documents. Total of 2 days.

Phase 1e

ISMS MANUAL & MANAGEMENT REVIEW

Clear Loop Security will ensure the information security management system (ISMS) is set up by providing an ISMS Manual which details specific activities to meet the requirements of ISO 27001; this will be tailored to the organisation. Clear Loop Security will also chair the first management review meeting (MRM), which is a mandatory item to demonstrate that the ISMS is operating, and provide minutes as well as a template for recording the output of future MRMs.

Output

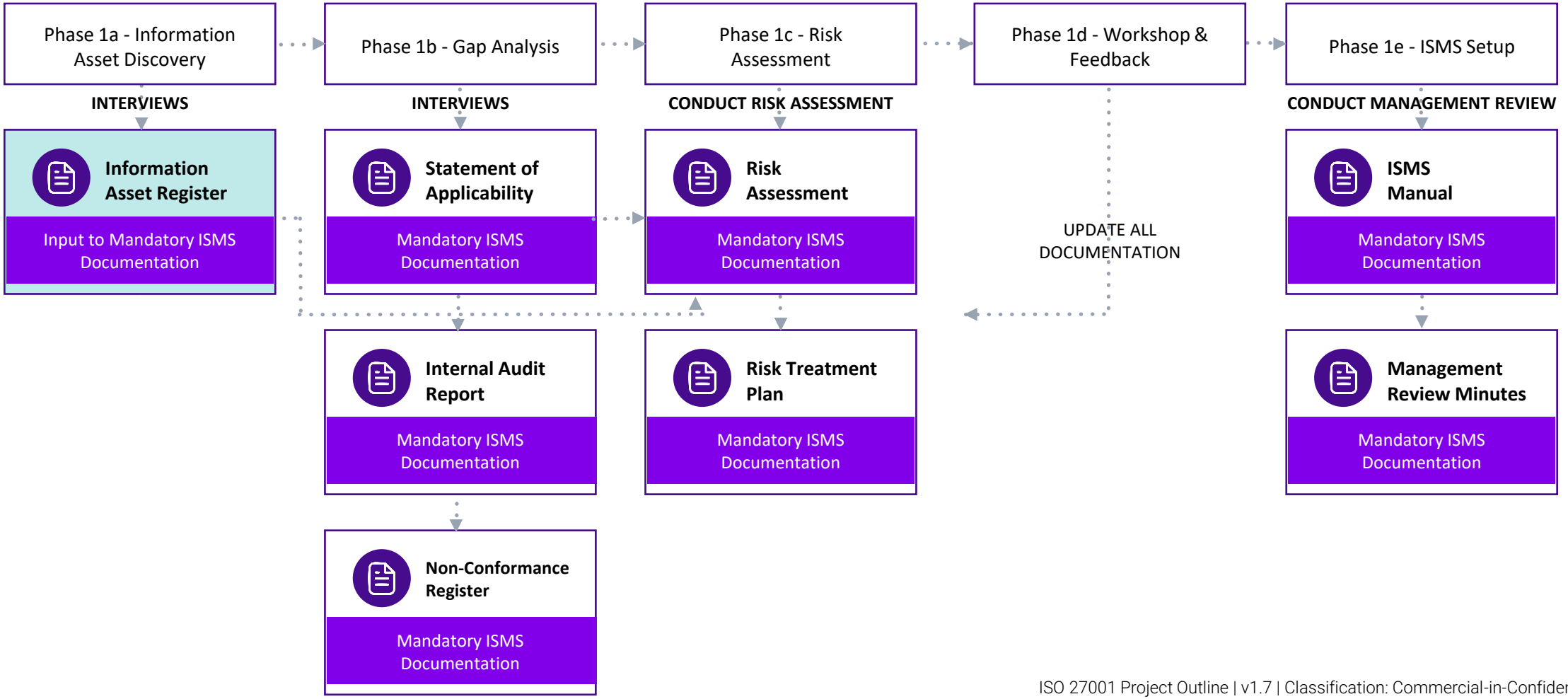
- ISMS Manual
- MRM minutes and template

Duration

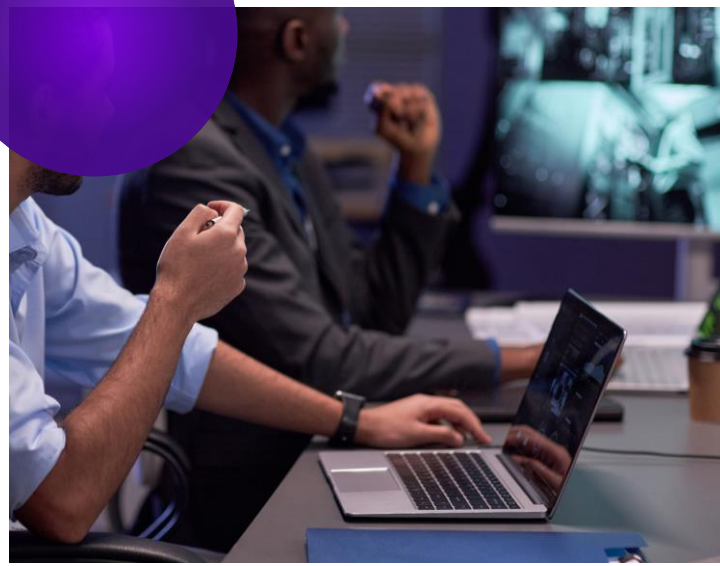
1 day for the ISMS Manual, 1 day for running the MRM and providing the minutes. Total of 2 days.

SUMMARY OF ACTIVITIES & OUTPUTS

The diagram below states the outputs of activities conducted in Phase 1, to show how this approach assists organisations in meeting their mandatory requirements for documented information under ISO 27001. The project is run in such a way that organisations will have made significant advances in setting up their Information Security Management System (ISMS) at the conclusion of this phase.



Phase 2 & 3 Activities



The effort required for these phases of the project depends on the outcome of the initial round of activity and how much work is required to address identified gaps and implement the management system. This will be informed by the roadmap that is agreed in the workshop at the end of Phase 1.

As each organisation differs in the amount of internal resource available to undertake ISO 27001 work, Clear Loop Security recommends using a call-off contract where a number of days are agreed in advance, but only billed as they are used. Specific activity will be agreed, including the number of days required, then this will be billed in arrears on a monthly basis as the days are consumed. Based on our experience of undertaking previous projects of this nature, the call-off element should usually be budgeted for around 20 days of effort.

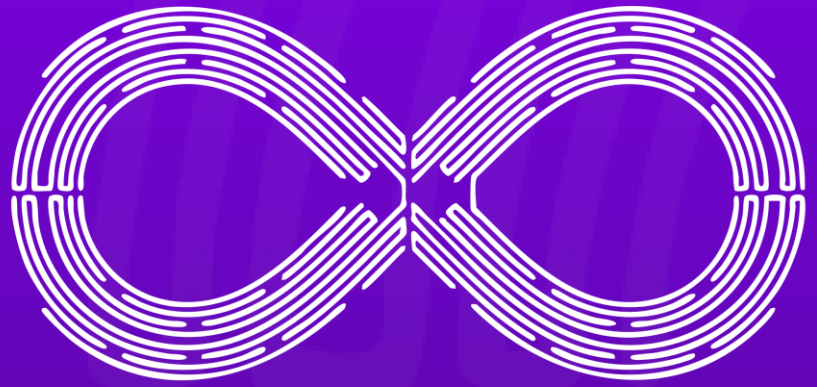
Certification Costs and Additional Costs

In addition to the effort required for Clear Loop Security to assist you with meeting the requirements of ISO 27001, there are costs for the certification body that will audit and certify you to the standard. We partner with a UKAS accredited certification body that will conduct your Stage 1 (verification) and Stage 2 (certification) audits.

During the initial engagement we will provide the certification body's scoping questionnaire to you, and obtain costs for these aspects. This will include not just the initial certification, but also annual surveillance audits to maintain your ISO 27001 certification for the first three year cycle.

We recommend that you purchase your own copy of ISO 27001 from BSI, and will direct you to obtain a copy of both ISO 27001 and ISO 27002 at the start of the project. The total cost of these as of April 2025 is around £400.

For maintenance of the ISMS we recommend the implementation of a dedicated GRC platform which will significantly reduce the effort to keep all controls and management activities up to date. Clear Loop Security also provides ongoing support to ensure that regular actions such as internal audits and management reviews take place in accordance with the standard. We will provide costs for these as required.



CLEAR LOOP SECURITY

clearloopsecurity.com