6clicks GRC Assessment Method

6clicks is a versatile platform that enables consultants and professionals to manage a wide variety of GRC activities including assessments and implementation of GRC programs based on many different frameworks and standards including ISO 27001, other ISO standards (Quality, Safety, Environment) and the NIST Cyber Security Framework, for starters.

In this guide, we will begin with a description of how to perform a fundamental bottom-up assessment against a single standard. We'll then work towards implementing a mature GRC program to enable an organization to conform with all relevant standards, and we'll do that by showcasing how you can add more value with a comprehensive top-down assessment leveraging 6clicks.

Conduct a fundamental (bottom-up) audit or assessment in 6clicks

The following steps explain how to conduct a black-and-white compliance-based audit or assessment against a single framework or standard using 6clicks:

1. Setup the relevant 6clicks team

If you're an advisor or consultant using 6clicks, you'll create a new client Spoke from your Hub team. If you're an internal GRC professional, make sure you're in the correct 6clicks team with the necessary permissions to use all the necessary modules.

2. Get Content from the Content Library

Navigate to the Content Library using the link at the top of the screen, then filter or search for the desired standard or framework (ISO or NIST). Let's start with items tagged as "Authority" documents although we could also search for a ready-made questionnaire tagged "Assessment" if we'd like to send the assessment to a third party to complete.

3. Begin your Audit or Assessment

Navigate to the Audit & Assessment module and choose to create a new "Requirement Based Assessment (RBA)" based on the selected "Authority" document. Define the fields you'd like to assess such as "Applicability" and "Implementation Status" and change the status of the assessment from Draft to Published.

4. Complete your Audit or Assessment response

For an RBA, go to the Responses tab and create a new response where you can define the answers to each field for each requirement. In the right-hand side panel, you can also quickly and easily add attachments, raise risks (and treatment plans) and issues (and actions), or see more information about the requirement if you need it.

5. Review the Audit & Assessment results

Once you've completed the data collection for your Audit or Assessment choose Submit. You can use Pixel Perfect to create a paginated report on the Reports tab or navigate to the Reporting & Analytics module to visualise the results. Export the reports or deliver the results directly via 6clicks including built-in presentations and stories.

6. Create and action a remediation plan

Be certain to take --and demonstrate-- action after running an assessment. Issues & Actions and/or Risks & Risk Treatment Plans raised during the assessment process are delivered via reporting and also directly in 6clicks as a live system for helping customers assign tasks and track remediation through to closure.

Add value as a part of comprehensive (top-down) audit or assessment in 6clicks

The following steps explain how to apply additional context, scoping, and top-down risk assessment to drive a risk-based approach to compliance and the adoption of controls using 6clicks:

1. Establish the scope and context

Take the time to understand the context of the assessment including industry, applicable compliance requirements and organisational size, as well as the scope of the assessment, i.e., whether it is for the entire organisation, or a particular system. The 6clicks Content Library includes templates to help establish the scope and context of an assessment.

2. Identify information assets, owners, and classifications

To help an organisation fully understand the scope and context, assist with the identification of information assets, owners and classifications including components and system boundaries (if necessary). Build an Information Asset Register in 6clicks to inform the identification of threats and risks in the next step.

3. Identify threats and risks

Perform a top-down analysis of the threats and risks using the 6clicks Risk module and Risk Libraries as a precursor to assessing compliance requirements and implementing requirements on a risk basis, or accepting risks that are tolerable. Link risks to causes, impacts, assets, existing control as well as risk treatment plans.

4. Run an Audit & Assessment of the selected controls

Run an Audit or Assessment against a standard or framework. With a risk assessment already completed, you can link requirements to risks that provide the rationale for adoption (an ISO 27001 requirement) or provide the associated risk assessment, risk treatment and/or risk acceptance where the requirement is justifiably unmet.

5. Review the Audit & Assessment results

As per the steps in the fundamental (bottom-up) GRC assessment method.

6. Raise Issues & Actions and/or Risks & Risk Treatment Plans

As per the fundamental (bottom-up) assessment, though you should already have risks on your risk register to refine.

Create and maintain a mature GRC program in 6clicks

Now, if not during earlier stages of assessment, you will establish the scope and context, identify information assets, identify & assess risks, select relevant internal controls, and may have executed some remediation through Issues & Actions or Risk and Risk Treatment Plans.

The next step in creating a mature GRC program is to develop a suite of policies and implement them. In 6clicks, this is achieved via the Control Sets module and provides your first line of defence before then relying on audits and assessments as your second line of defence.

1. Create one or more Control Sets

The good news is that 6clicks provides a suite of Control Sets in its Content Library, or alternatively you can import them or start from scratch. When you create a new control and link it to relevant requirements, 6clicks' Hailey AI can help compose succinct control statements that takes into consideration the applicable requirements.

2. Review and refine Responsibilities

The key aspect of Controls Sets is Responsibilities that define who and what, and optionally when and how often. 6clicks turns policies into actions that provide ongoing measurement of control effectiveness. Tasks are sent out to assigned members and evidence is attached. The evidence is then made available during Audits & Assessments.

3. Update your Audit & Assessment

Over time with evidence attached by assigned members to Responsibilities, you can update the Implementation Status of requirements in any Statement of Applicability or internal control assessments. The task information is available in the right-hand side panel where there is a link between the requirements and the control (Hailey AI can assist with that).

4. Conduct internal audit(s)

To achieve certification to ISO 27001 or for added assurance regardless of the standard you're following an independent audit or assessment against control or compliance requirements can be conducted in 6clicks. Return to the Audit & Assessment to carry out on audit or assessment against control or compliance requirements.

5. Hold a management review meeting

To gain management support and direction hold a management review meeting using the data in 6clicks and the presentation and story capability to explain the scope and context assessment, new/updated risks & risk treatment plans, new/updated policies and controls sets, results of the internal audit(s), and new/update issues & actions.

6. Undergo certification activities

Arrange for any external assessments including certification audits. In addition to reporting, the Trust Portal provides a useful mechanism for showcasing your Audit & Assessment results and policies / control sets to auditors performing documentation review, in addition to customers (or regulators) seeking assurance of your program.

We've expanded on each of these methods which include references to the 6clicks Knowledgebase and 6clicks Academy that can be found in playbooks you can get from the 6clicks Content Library.

6clicks includes a Third-party module providing the capability to maintain a list of your suppliers including any associated data such as contract manager, attachments like contracts, links between third parties and any assets with which they are associated, as well as the capability to send third-parties assessments as a part of your supply chain practices.