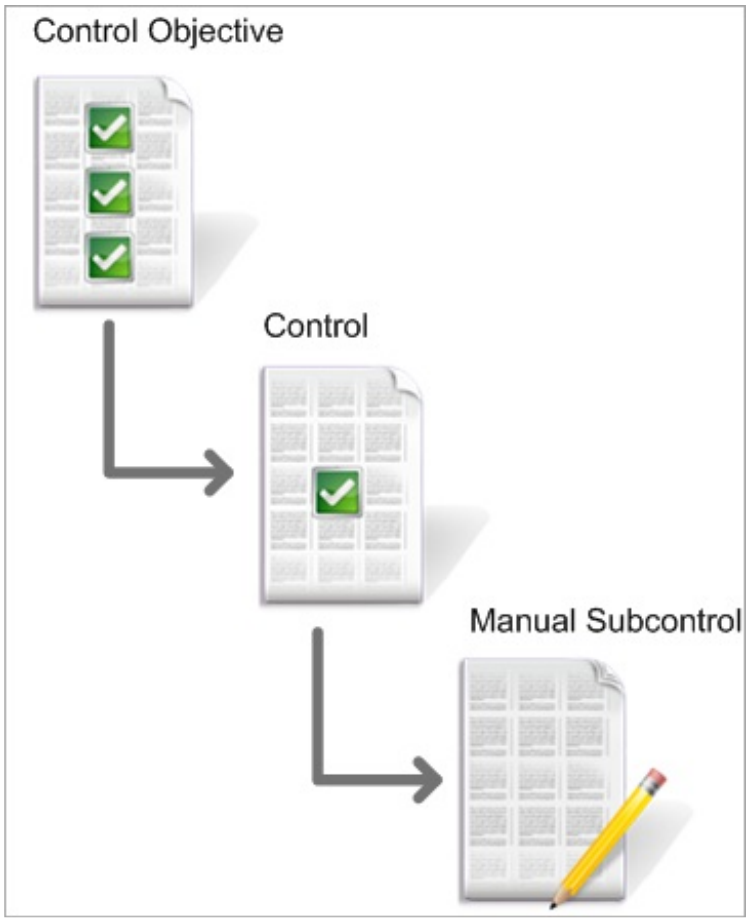
About Controls

Under any defined group, subgroup, or control content pack in **Organization Content**, you can create one or more new control objectives as a starting point to define one or more controls and subcontrols that address the new control objective.



The basic control objective structure.

Notes:

- See About Automatic Controls for more details on checks.
- **Control objectives**: State the desired result or purpose to be achieved by implementing control procedures in a particular process. Control objective titles display in the user questionnaire.

EXAMPLE

You have a high-level company policy that specifies:

"Access to information, information processing facilities, and business processes must be controlled on the basis of business and security

requirements. Access control rules must take account of control objectives and controls for information dissemination and authorization."

In that case, you might specify the following control objective:

"To ensure authorized user access and to prevent unauthorized access to information systems."

- **Controls:** Address an aspect of the control objective. Under any existing control objective in the **Organization Content** hierarchy, you can create one or more new controls, each of which specifies an action or process. The control title is the section title in user questionnaires.

EXAMPLE

You have the following control objective:

User Access: To ensure authorized user access and to prevent unauthorized access to information systems.

One of several controls you may put in place to support this objective might be to implement a user registration control. A statement of that control could be the following:

"There must be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services."

- **Subcontrols:** Specify a check or procedure used to enforce or evaluate compliance with the associated control. Under any existing control in the **Organization Content** hierarchy, you can create one or more subcontrols (either automatic or manual). The subcontrol question and choices display in the main pane of the user's questionnaires.

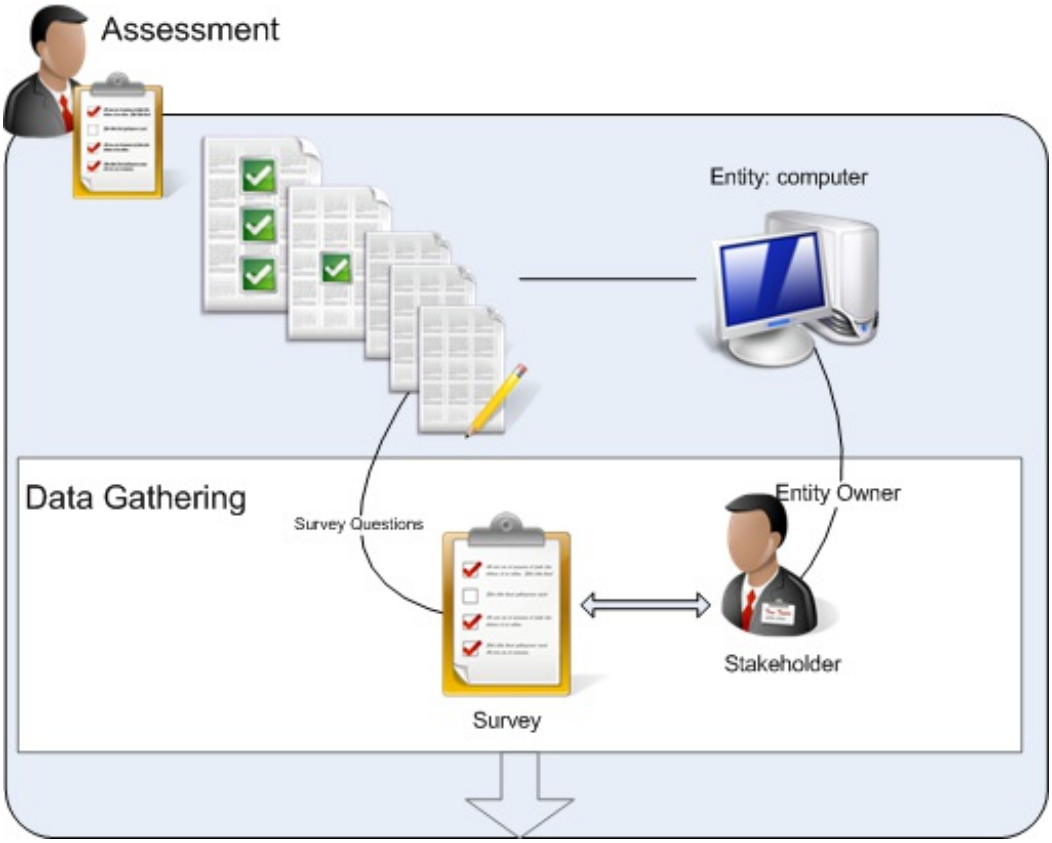
EXAMPLE

You have the following control:

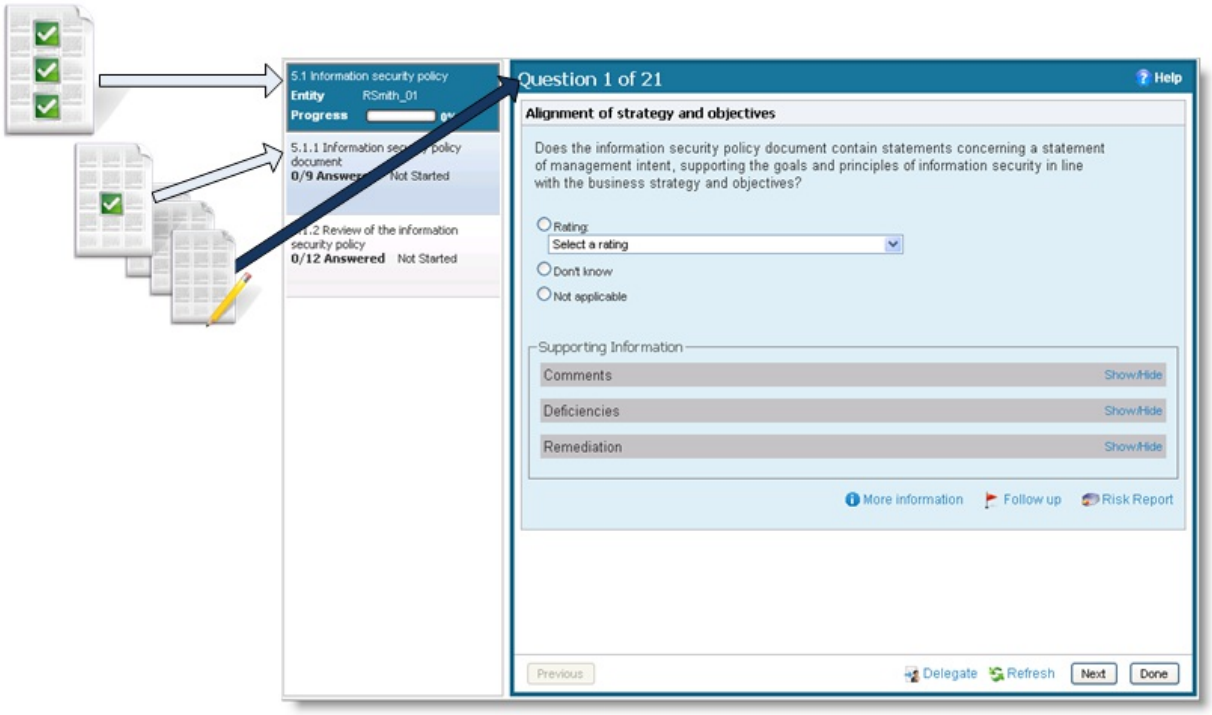
"There must be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services."

One of the subcontrols you may put in place to support or verify compliance with this control might be to check if there is a process in place and test the process to determine how well it works. To implement a subcontrol, you can specify automated tests of a control, or create questionnaire questions that can measure satisfaction with the control and control objectives.

You can assign control objectives or controls to entities in an assessment. If the subcontrol is manual - that is, if users provide answers to questions - the questionnaire is assigned to the entity owners identified as stakeholders of the information-gathering stage of the workflow process, as shown below:



The system produces a questionnaire from the object chosen in Selecting Controls and Questionnaires , where the highest level is the questionnaire title. The following example shows the questionnaire that is created when the program author selects the ISO-5.1 Control Objective and assigns it to an entity:



If the program author selected ISO-5.1.1 only, then the questionnaire title would be 5.1.1 Information security policy and the questionnaire would only contain the questions from the 5.1.1 subcontrols.