Understanding Controls and Questionnaires

Before jumping into the creation or customization of your own Organization's policy and control framework, it is important to have a basic understanding of terminology as well as the basic elements or components needed to build a policy and control "framework".

- **Policy and Control Framework or Group Hierarchy.** At the highest level in the policy, the hierarchy is the organization's policy or control "framework" or grouping hierarchy that groups high-level policies and control objectives. The grouping of control objectives can be based on or include the "domains" or broad categorization provided by standards-based frameworks such as CobiT, ISO 17799, PCI-DSS, NIST SP 800-53 or SP 800-66. For example, ISO 17799 has domains or categories that include such areas as security policy, system access control, computer and operations management, physical and environmental security, personnel security, entity classification, and control.

  The grouping hierarchy can also be of an organization's own design, such as defining a hierarchy of control objectives based on location, organizational structure, or stage of deployment. Or, you can combine both the hierarchy grouping reflecting the needs of your organization as well as take into account those of standards-based frameworks you wish to implement.

- **Content Packs.** Contains a group of control objectives, controls, and subcontrols, Questionnaires and topics, or Policy Documents for your organization that you want to develop using the same process and timeline.

- **Control Objectives.** Within the broader categories of a policy and control framework, policy and control objectives are statements that specify the objectives for developing and implementing controls (control checks or test procedures) that enforce, check, or verify compliance with higher level management goals and objectives. So, the control objective states the desired result or purpose to be achieved by implementing control procedures in a particular process. For, example, ISO 17799 specifies an Access Control domain to satisfy the high-level business requirement or policy to properly control access to information in an organization. So, the control objective, in this case, is that 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 policies and control objectives for information dissemination and authorization.

- **Controls**. The terms "Policy" and "Control" are often misunderstood. That is, they may be interpreted or have a different meaning to people from different backgrounds such as security, IT, regulatory compliance and auditing. In Resolver RiskVision, the terms "policy" or "control" means specific rules of behavior that can be enforced or verified either through automatically executed subcontrol checks and tests or responses to questionnaire questions distributed to business and technical owners, administrators, or other stakeholders for the relevant entities.

  For example, in the RiskVision Content Library hierarchy, under the ISO Section 11 "User Access Management" control objective, Resolver provides four unique controls, for user registration, privilege management, user password management, and review of user access rights. For each control, there can be many subcontrols that can be used to check conformance or compliance with the associated control.

- **Subcontrols.** For each Resolver control, users can define one or more sub-control checks implemented using automatically-run test procedures or manual control (questionnaire) questions. (For manual controls, questionnaire questions are distributed to the business owner or other parties (stakeholders) responsible for the associated entity(s).

  For example, in the RiskVision Content Library > Policies and Controls > Standards > ISO 17799 > 11 - Access Control > User Access Management hierarchy displayed in the RiskVision solution, the User Password Management control includes a half dozen or so manual control checks that enforce or verify compliance with the user password management control policy objectives.

- **Control Target Profiles**. Named collections of attribute values that define some group of entities as being similar for the purpose of choosing controls to evaluate and retrieve control results, since the entities matching the same profile have similar characteristics.