Understanding Configurations

Any assessments you run in RiskVision involve objects from on the **Configuration** menu. Objects may need to be configured differently for each assessment, depending on your business needs. The following objects must be configured before launching an assessment:

- Workflows;
- Escalations;
- Email Templates;
- Filters;
- Ownership Types;
- Assessment Configuration;
- Entity Configuration;
- Findings Configuration;
- Vulnerability Risk Configuration;
- Incident Configuration;
- Questionnaire Presentation Options; and
- Ticket Management Preferences.

The following describes how to configure some of the above options:

- **Workflows**: You can choose a workflow other than the default workflow using the assessment and policy creation wizards. If you want an exception, ticket, finding, and incident to follow a workflow pattern other than the default workflow, you must configure the selection criteria within those workflows. For more information on workflows, see the following topics:
  - About Workflows
  - Modifying Stage Settings
  - Specifying Multiple Workflows
- **Escalation**: Sent to the requestor, owner, or manager when a ticket is overdue. For more information, see Creating an Escalation Configuration and Managing Escalation Configurations .
- **Email Templates**: Used to notify stakeholders about an event. Several default email templates are available. If your organization prefers to follow a particular procedure for its internal communications, you can design an email template. For more information, see Configuring E-mail Templates .
- **Filters**: A set of conditions used by reports to match records, and by dynamic groups to limit membership, user access, and more. Filter types include Assessment, Dynamic Group, Entity, Exception Request, Incident, Program, Response, Risk, and others. For more information, see About Filters .
- **Ownership Types**: Ownership types link workflow stage stakeholders to the system users who are assigned to an entity or policy. This allows processes such as programs, tickets, and policy pack approvals to run automatically. You can restrict which user can be assigned as a type of owner based on the user's role assignment. For more information, see About Ownership Types .
- **Assessment Configuration, Entity Configuration, Findings Configuration, Vulnerability Risk Configuration, and Incident Configuration**: Depending on the RiskVision application, a common threshold range criteria can be established for assessments, findings, vulnerabilities, risks or incident objects. When assessments are run, the risk, vulnerability and incident scores are derived according to the default range. Before you run any assessment, ensure that the threshold range is configured according to the assessment objective and meets auditing guidelines and policies. For more information, see Configuring a Threshold

Range for Risk, Vulnerability and Incident Scores.

- **Ticket Management Preferences**: Configure your preferences for sending ticket escalations. For more information on setting the ticket preferences, see About Ticket Management Preferences .