

Compliance Risk Manager (CRM) - Data Sheet

Compliance Risk Manager (CRM) is an add-on module to Prevari's Technology Risk Manager (TRM). CRM provides the ability to refine TRM risk indices and models with the controls prescribed by regulations and standards. Today, CRM fully supports compliance with:

- ISO 17799/27002,
- PCI-DSS,
- SOX,
- CobiT,
- GLBA,
- DIACAP,
- NIST 800-53,
- HIPAA,
- Safe Harbor, and
- Custom Organizational Policies.

CRM enables the organization to understand the specific relationship between compliance and the risk of operating both compliant and non-compliant infrastructures.

By establishing a quantitative relationship between compliance and risk, one can precisely understand the specific impact of compliance to an organization's risk posture. Combined with the modeling features of TRM, CRM enables building detailed simulations and comparisons which inform decisions regarding how compliant is compliant enough. This detailed understanding better prepares an organization to educate and negotiate with internal and external auditors and assessors.

Audit fatigue is reduced by using CRM's web interface to distribute compliance questionnaires to the proper participants and to track completion of those questionnaires. CRM reporting capabilities answer the question, "how compliant are we" and, when combined with TRM risk metrics provide powerful predictive analytics to support superior decisions regarding the interdependencies of compliance and risk.

CRM functionality and the 17799/27002 ISO template ships with all TRM installations.

The screenshot shows the Prevari Technology Risk Manager (TRM) interface. The main window is titled "Compare Process and Bus Units - Technology Risk Manager (TRM)". The interface is divided into several sections:

- Compliance Set Management:** Includes buttons for "Create New..." and "Save As...".
- Question Sets:** A tree view showing various compliance standards:
 - GLBA
 - HIPAA 1996
 - ISO 17799:2005 (27002)
 - Risk Assessment & Treatment (selected)
 - Security Policy
 - Organization of Information Security
 - Asset Management
 - Human Resources Security
 - Physical & Environmental Security
 - Communications & Operations Mana
 - Access Control
 - Systems Acquisition, Development e
 - Information Security Incident Manag
 - Business Continuity
 - Compliance
 - NIST 800-53A
 - PCI - SAP 1.1
- ISO 17799:2005 (27002) : Risk Assessment _Treatment:** A detailed view of the questionnaire with columns for "Number", "Subsection", "Subsection ID", "Question", and "Answer".

Number	Subsection	Subsection ID	Question	Answer
03.001.001	Assessing security risks	4.1	Do risk assessments identify, quantify and prioritize risks against criteria for risk acceptance and objectives relevant to the organization?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
03.001.002	Assessing security risks	4.1	Do the risk assessment results guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
03.001.003	Assessing security risks	4.1	Is the process of assessing risks and selecting controls performed a number of times to cover different parts of the organization or individual information systems?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
03.001.004	Assessing security risks	4.1	Does the risk assessment include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation)?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
03.001.005	Assessing security risks	4.1	Are risk assessments performed periodically to address changes in the security requirements or changes to the risk situation, including assets, threats, vulnerabilities, impacts, risk evaluation and significant system or network changes?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
03.001.006	Assessing security risks	4.1	Are these risk assessments undertaken in a methodical manner capable of producing comparable and reproducible results?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
03.001.007	Assessing security risks	4.1	Does the information security risk assessment have a clearly defined scope, such as the whole organization, parts of the organization, an individual information system, specific system components, or services in order to be effective and include relationships with risk assessments in other areas, if appropriate?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
03.001.008	Treating security risks	4.2	Does the organization decide criteria for determining whether or not risks can be accepted before considering the treatment of a risk? Risks may be accepted if, for example, it is assessed that the risk is low or that the cost of treatment is not cost-effective for the organization.	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
03.001.009	Treating security risks	4.2	Are decisions to accept risks recorded?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
03.001.010	Treating security risks	4.2	Are risk treatment decisions made for each of the risks identified following the risk assessment?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
03.001.011	Treating security risks	4.2	Are one of the following possible options for risk treatment used: 1) applying appropriate controls to reduce the risks, 2) knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and criteria for risk acceptance, 3) avoiding risks by not allowing actions that would cause the risks to occur, or 4) transferring the associated risks to other parties, e.g., insurers or suppliers?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
03.001.012	Treating security risks	4.2	For those risks where the risk treatment decision has been to apply appropriate controls, are these controls selected and implemented to meet the requirements identified by a risk assessment?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A