Information Security Management

Discover why 50,000 professionals have switched to easy2comply™
Presentation Objective

- Provide an overview of our Information Security building blocks
- Offer insight into the look and feel of the application
- Showcase how you can easily use our software
Who Is it for?

- Our Information Security software has been designed with the needs of the Chief Information Security Officer in mind and can be used by:
  - Information Security Steering Committee
  - Information Security Managers
  - Information Technology Managers

- No project is too big or too small
  - It can be used by small groups (1 – 5 users) all the way up to the whole enterprise (10,000 users)

- Implementing our software has never been easier!
Information Security Management

- Assets and Units
- Threats and Controls Assessment
- Security Incidents
- Tasks, Notifications and Messages
- Reports and Management Dashboards
This is where you define your organizational tree. Our software combines a dual hierarchy: one for your assets, units and locations, and one for your information security activities and procedures.

You can also look at your tree horizontally across the enterprise. This feature allows you to drag and drop parts of your tree into simple structures to ease reporting and comparative analysis.
Assets and Units

Each item can be documented in terms of Owner, Type, Asset Value and Attachments.

Structure can be built with no limitation to the number of levels.
Threats and Controls Assessment

Assess your Threats using one or more of the available methodologies:
1) Impact vs. Likelihood Risk Square
2) Questionnaire

Identify your Threats within the Asset or Unit. Document, categorize and classify the vulnerabilities. Attach any supporting evidence to the risk record.

Mitigate your Threats by linking relevant controls to specific Threats. Check the controls for their level of effectiveness. Schedule the control checking process.
Assessment Flow

Identify
• Threats
• Risk Description
• Vulnerabilities

Assess
• Impact
• Likelihood
• Risk Score

Control
• Control Mapping
• Auditing
• Remediation
## Threat Identification

**Identify and assess all of the relevant Threats**

<table>
<thead>
<tr>
<th>Id</th>
<th>Threat</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Theft of media or documents</td>
<td>2.97</td>
</tr>
<tr>
<td>3</td>
<td>Disclosure</td>
<td>3.4</td>
</tr>
<tr>
<td>5</td>
<td>Corruption of data</td>
<td>1.77</td>
</tr>
<tr>
<td>6</td>
<td>Illegal processing of data</td>
<td>2.41</td>
</tr>
<tr>
<td>7</td>
<td>Error in use</td>
<td>2.97</td>
</tr>
<tr>
<td>8</td>
<td>Abuse of rights</td>
<td>1.85</td>
</tr>
<tr>
<td>9</td>
<td>Denial of actions</td>
<td>1.31</td>
</tr>
</tbody>
</table>
### General Details

| Risk Profile | Template | Threat |

### Qualitative Assessment

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. What is the level of classification of the impacted information asset?</td>
<td>Medium</td>
</tr>
<tr>
<td>2. What is the level of loss of confidentiality in case of an incident?</td>
<td>High</td>
</tr>
<tr>
<td>3. What is the level of loss of integrity in case of an incident?</td>
<td>Low</td>
</tr>
<tr>
<td>4. What is the level of loss of availability in case of an incident?</td>
<td></td>
</tr>
<tr>
<td>5. What is the level of impaired operations (internal or third parties)?</td>
<td></td>
</tr>
</tbody>
</table>

### Formula

\[(P^{0.4})(L^{0.6})\]

### Result

<table>
<thead>
<tr>
<th>Score</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4</td>
<td></td>
</tr>
</tbody>
</table>

### Vulnerabilities

- Incorrect dates: 10%
- Incorrect parameter set up: 10%
- Lack of back-up copies: 30%
- Lack of efficient configuration change: 20%
- No or insufficient software testing: 20%
- Well-known flaws in the software: 10%

**Assessment performed according the CIA-based questionnaire or Impact vs. Likelihood.**

**Vulnerabilities needs to be mapped to the relevant Threat.**
Control Mapping

Here you can see the Threat...

...together with the associated set of Controls mapped to the Threat.
Security Incidents

- Capture your Security Incidents and other Event Data across your Tree
- Assess the impact of the Incident and link each impact to your Threat and Control map
- Respond effectively to each Incident, draw relevant conclusions and allocate Actions accordingly
Incident Management

- What
- When
- Where

- Multiple Impacts
- Total Damage
- Indirect Impacts

- Improvement Plan
- Controls
Incidents

<table>
<thead>
<tr>
<th>Name</th>
<th>Report Date</th>
<th>Unit + Process</th>
<th>Open/Close</th>
<th>Type</th>
<th>Incident Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malfunctioning in the network</td>
<td>09/05/2010</td>
<td>Cisco Router</td>
<td>Opened</td>
<td>First</td>
<td></td>
</tr>
<tr>
<td>Power failure in servers room</td>
<td>24/04/2010</td>
<td>Servers Room</td>
<td>Opened</td>
<td>First</td>
<td></td>
</tr>
<tr>
<td>Theft of sensitive docs</td>
<td>09/05/2010</td>
<td>PeopleSoft CRM</td>
<td>Opened</td>
<td>First</td>
<td></td>
</tr>
</tbody>
</table>
Assign the failed Controls, investigate the event and analyze the reasons why the Controls were insufficient in preventing this from happening.

The narrative and the investigation:

Early Saturday morning, the main generator switch incurred some type of fault, which resulted in a fire. The sprinkler system was immediately activated, and according to the Fire Battalion Chief, water was also used in putting out the fire.

The location of electrical fault resulted in a failure of not only the UPS system, but also the cooling system. Temperatures inside the facility were over 38C by the time some of the servers owners were able to assess the damage, which in some cases was a total loss of both machine and data.

There is currently no ETA for resolution as several of the circuits involved have to be not only recreated, but rewired from scratch once the damaged circuits are removed from the melted and charred building. The latest information we have is that servers were starting to come back online as of Sunday morning.
Create and follow up on Actions:
1. Link Actions to your Control
2. Each Action has an Owner and a Due Date for follow up
3. New Messaging feature

Define your own Alerts (for example):
1. Missed Due Dates
2. Approaching audits
3. Changes to your data

Notifications are sent directly to your email inbox with a link taking you to the software
Tasks Management

All Actions and Tasks are listed under the Organization’s Action Plan. Actions are listed according to status, owner and due date.

An individual action can contain multiple sub-tasks, each allocated to a different owner with a different due date.
Notifications and Messages

These notifications are delivered directly into the user’s email.

Software comes with the ability to generate reminders, alerts and notifications regarding Action Plan due dates and scheduled control tests.
Reports and Dashboards

**Built-in Reports** are pre-defined report templates that can be generated and exported to multiple file formats.

**Management Dashboards** are colorful and interactive charts generated by our powerful charting engine.

**Excel Reports** are templates created by the User that define precisely the data wanted to be seen.

---

Reports and Management Dashboards
Built-in Reports
Dashboards
Information Security Management

Assets and Units

Threats and Controls Assessment

Security Incidents

Tasks, Notifications and Messages

Reports and Management Dashboards
Thank you

For more information, please contact:

Sales@checkpoint.com