Applied Security Visualization

Color Gallery

Figure 3-1

Figure 3-17
Figure 4-11

Figure 4-12
Figure 6-12

Figure 6-13
Figure 6-16

Figure 6-17
### Control Objectives

<table>
<thead>
<tr>
<th>User Account Management</th>
<th>Establish firewall configuration standards</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Management</strong></td>
<td><strong>Change Management</strong></td>
</tr>
<tr>
<td>Use identification to authorize access to IT computing</td>
<td>Approving changes to firewall configuration</td>
</tr>
<tr>
<td>Use authentication to allow access to IT computing</td>
<td>Establish least privilege access to data</td>
</tr>
<tr>
<td>Secure online access to data</td>
<td>Secure network diagram</td>
</tr>
<tr>
<td>Implement access control for dial-up connections</td>
<td>Monitor configuration standards for firewalls</td>
</tr>
</tbody>
</table>

**New Accounts**
- Procedures for requesting user accounts
- Procedures for issuing user accounts
- Procedures for suspending user accounts

**Review**
- Procedures for establishing user accounts
- Management Review of User Accounts
- Management Confirmation of access rights
- Comparison of resources with recorded accountability

**Firewall Configuration**
- Deny all traffic from untrusted networks/hosts
- Deny connections between publicly accessible systems
- Restricting inbound Internet traffic to DMZ
- Other protocols required by the business

**External Net**
- Approving external network connections
- Testing external network connections

**Requirements**
- List of services/ports necessary for business
- Justification and documentation for any available protocols

**Justification**
- Access Control Description

---

**Figure 7-6**

[Diagram of network configuration]

**Figure 8-6**

[Map of Europe with network connections]
Figure 8-19
Figure 8-23
Figure 8-24