The Procurement Checker
Anne-Marie Eklund Löwinder
.SE
Who?

• The Procurement Check was created as an initiative of the company Cybercom (www.cybercom.com)
• The purpose is to assist companies and organizations to set security requirements when procuring new systems
What?

• a process for managing practical tender requirements regarding information and IT security
• The instructions addressed to the purchaser or the project manager for a tender process are easy to follow
Why?

• The procurement checker works from an efficiency point of view.

• Systems are, always, in any of the following phases of the system life cycle:
  1) Decision to invest, procure or design a system in line with business requirements
  2) The system is being implemented
  3) The system is in use
  4) The system is being phased out

• The earlier in the process the security work is started, the higher level of efficiency is achieved
Step 1 - screen requirements and specify dimensions
Step 2 - sort and prioritize remaining requirements
Step 3 - Establish the project with its sponsor
Step 4 - Insert SHALL and SHOULD requirements in the tender's main document and rearrange the spreadsheet
Step 5 - Attach the spreadsheet to your tender documentation
Step 6 - Evaluate the tenders
Want to help?

• The set of security checkpoints will be managed over time. There are two main methods to gain input to this process.

  1) E-mail to upphandlingskollen@cybercom.com
  2) Semi-annual seminars for exchange of experiences, sign up by e-mailing upphandlingskollen@cybercom.com.

Please note that the seminars have an entry requirement: the attendees must have used the Procurement Check in a tender. The purpose of the seminars is to discuss practical experiences, not hypothetical situations of an academic nature.
What’s in it for you?

- It’s more expensive with a secure system.
- It's always faster to cut corners.
- The attitude "security is implicitly required, it should not need to be spelled out in the requirements" has time after time proven to be wrong.
- The more general questions, often called "best practice", are frequently forgotten.
- All suppliers that compete in a tender process are given the same conditions.
Layout

- Chapter/topic
- Checkpoint, security requirement
- Area (application, OS, DB, HW)
- Level (shall, should, question, disregard)
- Supplier declaration
- Detailed description to the supplier
Topics

• Physical Security
• Access and authorization
• Traceability and monitoring
• Network
• Encryption
• Security responsibilities of the supplier
• Backup and continuity
• Applications
• Resistance to attacks
• Documentation
<table>
<thead>
<tr>
<th>Details and comments from the supplier</th>
<th>Detailed description to the supplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sufficient burglar alarm has been installed in the offered physical operating environment.</td>
<td>Describe the solutions for burglar alarm, entrance control system and/or camera surveillance system (CCTV) and the maintenance thereof.</td>
</tr>
<tr>
<td>Access control systems provide functionality to follow-up of both successful and unsuccessful attempts at physical access. Logs are checked at least monthly, as part of the supplier’s commitment.</td>
<td>Describe in detail how the access control system handles failed attempts at physical access and what possibilities exists to subsequently monitor physical access to systems or information assets covered by this tender.</td>
</tr>
<tr>
<td>The operational environment is patrolled by guard. The patrolling occurs at irregular intervals, at least twice every 24 hours.</td>
<td>Account for what actions that have been taken for manual supervision of systems and other information assets that are part of the offered operational environment.</td>
</tr>
<tr>
<td>The supplier ensures that only authorized persons can be granted physical access to the systems that are part of the operating delivery.</td>
<td>In detail, account for the routines assuring that unauthorized persons doesn’t gain physical access to systems and other information assets that are part of the offered operational environment, even though they have legitimate access to the physical environment, e.g., data centers, office spaces.</td>
</tr>
<tr>
<td>The supplier’s offered solution has no restrictions based on other parties’ demands on shared resources such as IT environment, premises, or the like.</td>
<td>Account for whether other clients to the supplier shares the same technical infrastructure. If so, please describe how to ensure that no other client service requests lowers security or availability of the offered IT environments.</td>
</tr>
<tr>
<td>The purchaser is held non-liable by the supplier for damage caused by fire, moist, water and other environmental disaster scenarios (force majeure).</td>
<td>Account for methods and technical countermeasures for managing and mitigating damages caused by fire, moist, water or other disaster scenarios (force majeure related).</td>
</tr>
<tr>
<td>The solution provided by the supplier contains a solution for physical redundancy.</td>
<td>Describe solutions for ‘hot standby’, ‘cold standby’ or other methods/solutions on which the supplier has based its capacity to mitigate physical risks. Account for residual ‘single points of failure’.</td>
</tr>
</tbody>
</table>
Thank you!
amel@iis.se
@amelsec