“Common criteria vs. ISO 27001”
jean-yves.bernard@thalesgroup.com

- **Development environment in a CC evaluation (DVS)**
  - Developer point of view
  - Evaluator point of view

- **Information security management system (ISMS) and Risk Analysis**
  - Why an ISMS can be helpful to fulfill CC requirements?
  - Example (risk assessment/treatment)

- **ISO/IEC 27001:2005 certified ISMS**
  - Method to achieve an optimized CC DVS evaluation
  - Gain on evaluation workload

- **Conclusion**
Introduction

- **Convenor:** Jean-Yves BERNARD
  - Evaluator for 8 years
  - Thales ITSEF technical manager
  - Lead auditor ISO/IEC 27001:2005 (certified by LSTI)
  - Risk manager ISO/IEC 27005:2008 (certified by LSTI)

Thales ITSEF:
- HW & embedded SW ITSEF
- Under ANSSI agreement
Target Of Evaluation Life cycle
Target Of Evaluation Life cycle

- TOE spec
- TOE dev
- TOE testing
- TOE personalisation
- End usage
Target Of Evaluation Life cycle

- TOE spec
- TOE dev
- TOE testing
- TOE personalisation
- End usage

« Evaluated » Development environment
Target Of Evaluation Life cycle

- TOE spec
- TOE dev
- TOE testing
- TOE personalisation
- End usage

« Evaluated » Development environment

« Not evaluated » (covered by guidance)
Target Of Evaluation Life cycle

« Evaluated » Development environment

- TOE spec
- TOE dev
- TOE testing
- TOE personalisation
- End usage

« Not evaluated » (covered by guidance)

Confidentiality of sensitive information
ALC_DVS, ALC_DEL
Development environment in a CC evaluation

Target Of Evaluation Life cycle

- TOE spec
- TOE dev
- TOE testing
- TOE personalisation
- End usage

« Evaluated » Development environment

- Confidentiality of sensitive information
  ALC_DVS, ALC_DEL

- Integrity of the TOE
  ALC_DVS, ALC_DEL, ALC_CMC

« Not evaluated » (covered by guidance)
**Target Of Evaluation Life cycle**

- **TOE spec**
- **TOE dev**
- **TOE testing**
- **TOE personalisation**
- **End usage**

**« Evaluated » Development environment**

- Confidentiality of sensitive information
  - ALC_DVS, ALC_DEL
- Integrity of the TOE
  - ALC_DVS, ALC_DEL, ALC_CMC

**« Not evaluated » (covered by guidance)**
Developer point of view (1/2)
Developer point of view (1/2)

- How can I know if I am ready?
Developer point of view (1/2)

- How can I know if I am ready?

Perform a review of the CC requirements
Developer point of view (1/2)

- How can I know if I am ready?
- Focus on ALC_DVS:
  “The developer shall produce and provide development security documentation”.

Perform a review of the CC requirements
Developer point of view (1/2)

- How can I know if I am ready?
- Focus on ALC_DVS:
  “The developer shall produce and provide development security documentation”. ALC_DVSx.1D
  ... documentation shall describe all the ... security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation... ALC_DVSx.1C

Perform a review of the CC requirements
**Developer point of view (1/2)**

- How can I know if I am ready?
- Focus on ALC_DVS:
  “The developer shall produce and provide development security documentation”. ALC_DVSx.1D
  ... documentation shall describe all the ... security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation... ALC_DVSx.1C

- There is no method that completely helps a developer to build its development security documentation.
- Even if the CEM can be used as a guidance, it is not sufficient to help the developer.
  - ALC_DVS.2–2
Developer point of view (1/2)

- How can I know if I am ready?
- Focus on ALC_DVS:
  "The developer shall produce and provide development security documentation". ALC_DVSx.1D
  ... documentation shall describe all the ... security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation... ALC_DVSx.1C

- There is no method that completely helps a developer to build its development security documentation.
- Even if the CEM can be used as a guidance, it is not sufficient to help the developer.
  - ALC_DVS.2–2

"I send all that I have to the evaluator and he will tell me if it is OK or not"
Developer point of view (1/2)

- How can I know if I am ready?
- Focus on ALC_DVS:
  “The developer shall produce and provide development security documentation”. ALC_DVSx.1D
  ... documentation shall describe all the ... security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation... ALC_DVSx.1C

- There is no method that completely helps a developer to build its development security documentation.
- Even if the CEM can be used as a guidance, it is not sufficient to help the developer.
  - ALC_DVS.2–2

“I send all that I have to the evaluator and he will tell me if it is OK or not”
Developer point of view (2/2)

- Important risk of several iterations in the evaluation process.
Developer point of view (2/2)

- Important risk of several iterations in the evaluation process increased by environment “complexity”.

- TOE development environment scope.
Evaluator point of view (1/2)
Evaluator point of view (1/2)

Focus on ALC_DVS: "ALC_DVSx–1: The evaluator determines what is necessary by first referring to the ST for any information that may assist in the determination of necessary protection..."
Evaluator point of view (1/2)

Focus on ALC_DVS: "ALC_DVSx-1: The evaluator determines what is necessary by first referring to the ST for any information that may assist in the determination of necessary protection..."
Evaluator point of view (1/2)

Focus on ALC_DVS: "ALC_DVSx-1: The evaluator determines what is necessary by first referring to the ST for any information that may assist in the determination of necessary protection..."

What Is necessary
Evaluator point of view (1/2)

Focus on ALC_DVS:  "ALC_DVSx-1: The evaluator determines what is necessary by first referring to the ST for any information that may assist in the determination of necessary protection."

Actually, it is very difficult to determine “what is necessary”
Evaluator point of view (1/2)

Focus on ALC_DVS: "ALC_DVSx–1: The evaluator determines what is necessary by first referring to the ST for any information that may assist in the determination of necessary protection."

- Actually, it is very difficult to determine “what is necessary”
- The evaluator implicitly has to perform a development environment vulnerability analysis
Evaluator point of view (1/2)

Focus on ALC_DVS: “ALC_DVSx–1: The evaluator determines what is necessary by first referring to the ST for any information that may assist in the determination of necessary protection.”

- Actually, it is very difficult to determine “what is necessary”
- The evaluator implicitly has to perform a development environment vulnerability analysis
Evaluator point of view (2/2)

- The CEM is generic, therefore evaluation work load is very impacted.
Other “issues”
Other “issues”

- CC do not require that a risk assessment is to be performed
  - But CC require some elements that are outputs of a risk assessment approach
    - Security measures
    - Sufficiency analysis (DVS.2 level).
Other “issues”

- CC do not require that a risk assessment is to be performed
  - But CC require some elements that are outputs of a risk assessment approach
    - Security measures
    - Sufficiency analysis (DVS.2 level).

- An Information Security Management System (ISMS) is not required
  - But CC indirectly require a security policy $\leq$ ALC_DVS. 2–3
    - A security policy not managed by a recognized ISMS and not validated by the management could be not relevant.
Information Security Management System solution...

- Stakeholders
- Requirements
- Stakeholders satisfaction
- Management system
  - Policy
  - Organizational controls
  - Technical controls
  - Objectives
An Information Security Management System (that respects a set of defined conditions) can be a «tool» that helps to correctly answer to DVS criteria.

**Information Security Management System solution**...
Risk Analysis solution...
A risk analysis performed in the scope of an ISMS (that respects a set of defined conditions) can also be a « tool » that helps to correctly answer to DVS criteria.
Example:
Example:
Example:

- An organization (company) develops a product and wants to obtain a certificate according to CC EAL4+ (DVS.2 and VAN.5 level).
Example:

- An organization (company) develops a product and wants to obtain a certificate according to CC EAL4+ (DVS.2 and VAN.5 level).
Example:

- An organization (company) develops a product and wants to obtain a certificate according to CC EAL4+ (DVS.2 and VAN.5 level).

- The company has an ISMS:
Example:

- An organization (company) develops a product and wants to obtain a certificate according to CC EAL4+ (DVS.2 and VAN.5 level).

- The company has an ISMS:
  - The TOE is developed in the scope of this ISMS.
  - The company has an ISMS policy that takes into account the fact that products are under CC evaluation.
  - The company ISMS answers to ISO/IEC 27001:2005 requirements.
ISO 27001 provides the requirements that must be implemented by an ISMS. If these requirements are respected, this means first that the ISMS is correctly established.
ISO 27001 provides the requirements that must be implemented by an ISMS. If these requirements are respected, this means first that the ISMS is correctly established.

**RISK assessment / treatment**
The company has performed a risk assessment with an identified methodology: 27005

ISO/IEC 27001:2005 4.2.1 c) 1)
The company has performed a risk assessment
- with an identified methodology: 27005
  ➔ ISO/IEC 27001:2005 4.2.1 c) 1)
- with defined risk acceptance criteria
  • The risk criteria take into account the fact that product under CC evaluation are developed in the scope of the ISMS
  ➔ ISO/IEC 27001:2005 4.2.1 c) 2)
Risk identification & Risk evaluation is taken into account (especially attacker level)

⇒ ISO/IEC 27001:2005 4.2.1 d) & e)
Risk identification & Risk evaluation is taken into account (especially attacker level)

ISO/IEC 27001:2005 4.2.1 d) & e)

asset
Risk identification & Risk evaluation is taken into account (especially attacker level)

ISO/IEC 27001:2005 4.2.1 d) & e)
Risk identification & Risk evaluation is taken into account (especially attacker level)

- ISO/IEC 27001:2005 4.2.1 d) & e)
Risk identification & Risk evaluation is taken into account (especially attacker level)

⇒ ISO/IEC 27001:2005 4.2.1 d) & e)
Risk identification & Risk evaluation is taken into account (especially attacker level)

⇒ ISO/IEC 27001:2005 4.2.1 d) & e)
Risk identification & Risk evaluation is taken into account (especially attacker level)

ISO/IEC 27001:2005 4.2.1 d) & e)
Risk identification & Risk evaluation is taken into account (especially attacker level)

⇒ ISO/IEC 27001:2005 4.2.1 d) & e)

- Asset
- Supportive asset
- Vulnerability
- Threats
- Incident scenario
- Risk

consequence => Asset value + C,I impact
CC (ST/PP) are taken into account
Risk identification & Risk evaluation is taken into account (especially attacker level)

⇒ ISO/IEC 27001:2005 4.2.1 d) & e)

- Vulnerability
  - Threats
    - Incident scenario
      - Risk

- Asset
  - Supportive asset

Consequence => Asset value + C,I impact
CC (ST/PP) are taken into account

Likelihood (VAN.5 level)
**Risk identification & Risk evaluation**

CC evaluation is taken into account (especially attacker level)

ISO/IEC 27001:2005 4.2.1 d) & e)

- **Asset**
- **Supportive asset**
- **Vulnerability**
- **Threats**
- **Incident scenario**
- **Risk**

Consequence => Asset value + C,I impact

CC (ST/PP) are taken into account

Likelihood (VAN.5 level)
Risk identification & Risk evaluation is taken into account (especially attacker level)

➔ ISO/IEC 27001:2005 4.2.1 d) & e)

- Asset
- Supportive asset
- Vulnerability
- Threats
- Incident scenario
- Risk
- Risk level
- Consequence => Asset value + C,I impact
- CC (ST/PP) are taken into account
- Likelihood (VAN.5 level)

Risk level = Risk level
Example risk evaluation criteria (chosen by the risk “manager”)
Example risk evaluation criteria (chosen by the risk manager)

- Level of risk is estimated

- ISO/IEC 27001:2005 4.2.1 e) 3)
- ISO/IEC 27005:2008 8.2.2.3
### Example risk evaluation criteria (chosen by the risk “manager”)

- Level of risk is estimated

```plaintext
ISO/IEC 27001:2005 4.2.1 e) 3)
ISO/IEC 27005:2008 8.2.2.3
```

<table>
<thead>
<tr>
<th>consequence (Asset value + C,I impact)</th>
<th>threat likelihood (considering VAN.5 level)</th>
<th>ease of vulnerability exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = no consequence on TOE dev</td>
<td>1 = low</td>
<td>1 = very hard (above VAN.5 level)</td>
</tr>
<tr>
<td>2 = med on TOE dev</td>
<td>2 = med</td>
<td>2 = hard (VAN.5 level)</td>
</tr>
<tr>
<td>3 = high on TOE dev</td>
<td>3 = high</td>
<td>3 = easy (under VAN.5 level)</td>
</tr>
</tbody>
</table>
## Example risk evaluation criteria (chosen by the risk “manager”)

- Level of risk is estimated

→ ISO/IEC 27001:2005 4.2.1 e) 3)
→ ISO/IEC 27005:2008 8.2.2.3

<table>
<thead>
<tr>
<th>consequence (Asset value + C,I impact)</th>
<th>threat likelihood (considering VAN.5 level)</th>
<th>ease of vulnerability exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = no consequence on TOE dev</td>
<td>1 = low</td>
<td>1 = very hard (above VAN.5 level)</td>
</tr>
<tr>
<td>2 = med on TOE dev</td>
<td>2 = med</td>
<td>2 = hard (VAN.5 level)</td>
</tr>
<tr>
<td>3 = high on TOE dev</td>
<td>3 = high</td>
<td>3 = easy (under VAN.5 level)</td>
</tr>
</tbody>
</table>
Example risk evaluation criteria (chosen by the risk “manager”)

- level of risk is estimated

- ISO/IEC 27001:2005 4.2.1 e) 3)
- ISO/IEC 27005:2008 8.2.2.3

<table>
<thead>
<tr>
<th>consequence (Asset value + C,I impact)</th>
<th>threat likelihood (considering VAN.5 level)</th>
<th>ease of vulnerability exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = no consequence on TOE dev</td>
<td>1 = low</td>
<td>1 = very hard (above VAN.5 level)</td>
</tr>
<tr>
<td>2 = med on TOE dev</td>
<td>2 = med</td>
<td>2 = hard (VAN.5 level)</td>
</tr>
<tr>
<td>3 = high on TOE dev</td>
<td>3 = high</td>
<td>3 = easy (under VAN.5 level)</td>
</tr>
</tbody>
</table>
Example risk evaluation criteria (chosen by the risk “manager”)

- level of risk is estimated

ISO/IEC 27001:2005 4.2.1 e) 3)
ISO/IEC 27005:2008 8.2.2.3

<table>
<thead>
<tr>
<th>consequence (Asset value + C,I impact)</th>
<th>threat likelihood (considering VAN.5 level)</th>
<th>ease of vulnerability exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = no consequence on TOE dev</td>
<td>1 = low</td>
<td>1 = very hard (above VAN.5 level)</td>
</tr>
<tr>
<td>2 = med on TOE dev</td>
<td>2 = med</td>
<td>2 = hard (VAN.5 level)</td>
</tr>
<tr>
<td>3 = high on TOE dev</td>
<td>3 = high</td>
<td>3 = easy (under VAN.5 level)</td>
</tr>
</tbody>
</table>
**Example risk evaluation criteria** *(chosen by the risk “manager”)*

The level of risk is estimated

ISO/IEC 27001:2005 4.2.1 e) 3)
ISO/IEC 27005:2008 8.2.2.3

<table>
<thead>
<tr>
<th>consequence (Asset value + C,I impact)</th>
<th>threat likelihood (considering VAN.5 level)</th>
<th>ease of vulnerability exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = no consequence on TOE dev</td>
<td>1 = low</td>
<td>1 = very hard (above VAN.5 level)</td>
</tr>
<tr>
<td>2 = med on TOE dev</td>
<td>2 = med</td>
<td>2 = hard (VAN.5 level)</td>
</tr>
<tr>
<td>3 = high on TOE dev</td>
<td>3 = high</td>
<td>3 = easy (under VAN.5 level)</td>
</tr>
</tbody>
</table>
**Example risk evaluation criteria** *(chosen by the risk “manager”)*

Level of risk is estimated

- ISO/IEC 27001:2005 4.2.1 e) 3)
- ISO/IEC 27005:2008 8.2.2.3

<table>
<thead>
<tr>
<th>consequence (Asset value + C,I impact)</th>
<th>threat likelihood (considering VAN.5 level)</th>
<th>ease of vulnerability exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = no consequence on TOE dev</td>
<td>1 = low</td>
<td>1 = very hard (above VAN.5 level)</td>
</tr>
<tr>
<td>2 = med on TOE dev</td>
<td>2 = med</td>
<td>2 = hard (VAN.5 level)</td>
</tr>
<tr>
<td>3 = high on TOE dev</td>
<td>3 = high</td>
<td>3 = easy (under VAN.5 level)</td>
</tr>
</tbody>
</table>
**Example risk evaluation criteria** *(chosen by the risk “manager”)*

- level of risk is estimated

- ISO/IEC 27001:2005 4.2.1 e) 3)
- ISO/IEC 27005:2008 8.2.2.3

<table>
<thead>
<tr>
<th>consequence (Asset value + C,I impact )</th>
<th>threat likelihood (considering VAN.5 level)</th>
<th>ease of vulnerability exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = no consequence on TOE dev</td>
<td>1 = low</td>
<td>1 = very hard (above VAN.5 level)</td>
</tr>
<tr>
<td>2 = med on TOE dev</td>
<td>2 = med</td>
<td>2 = hard (VAN.5 level)</td>
</tr>
<tr>
<td>3 = high on TOE dev</td>
<td>3 = high</td>
<td>3 = easy (under VAN.5 level)</td>
</tr>
</tbody>
</table>

*Risk = consequence * threat likelihood * ease of vulnerability exploitation*
Example risk evaluation criteria (chosen by the risk "manager")

- Level of risk is estimated

ISO/IEC 27001:2005 4.2.1 e) 3)
ISO/IEC 27005:2008 8.2.2.3

<table>
<thead>
<tr>
<th>consequence (Asset value + C,I impact)</th>
<th>threat likelihood (considering VAN.5 level)</th>
<th>ease of vulnerability exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = no consequence on TOE dev</td>
<td>1 = low</td>
<td>1 = very hard (above VAN.5 level)</td>
</tr>
<tr>
<td>2 = med on TOE dev</td>
<td>2 = med</td>
<td>2 = hard (VAN.5 level)</td>
</tr>
<tr>
<td>3 = high on TOE dev</td>
<td>3 = high</td>
<td>3 = easy (under VAN.5 level)</td>
</tr>
</tbody>
</table>

Risk = consequence * threat likelihood * ease of vulnerability exploitation

Focus on risk acceptance criteria
Example risk evaluation criteria (chosen by the risk “manager”)

- Level of risk is estimated

ISO/IEC 27001:2005 4.2.1 e) 3)
ISO/IEC 27005:2008 8.2.2.3

<table>
<thead>
<tr>
<th>consequence (Asset value + C,I impact)</th>
<th>threat likelihood (considering VAN.5 level)</th>
<th>ease of vulnerability exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = no consequence on TOE dev</td>
<td>1 = low</td>
<td>1 = very hard (above VAN.5 level)</td>
</tr>
<tr>
<td>2 = med on TOE dev</td>
<td>2 = med</td>
<td>2 = hard (VAN.5 level)</td>
</tr>
<tr>
<td>3 = high on TOE dev</td>
<td>3 = high</td>
<td>3 = easy (under VAN.5 level)</td>
</tr>
</tbody>
</table>

Risk = consequence * threat likelihood * ease of vulnerability exploitation

Focus on risk acceptance criteria

ISO/IEC 27001:2005 4.2.1 e) 4)

In our case, threshold is: 2*2*2 = 8 (take into account CC)

risk acceptance criteria is « risk < 8 ».
**Example risk evaluation criteria** *(chosen by the risk “manager”)*

- A level of risk is estimated

  ➤ **ISO/IEC 27001:2005 4.2.1 e) 3)**
  ➤ **ISO/IEC 27005:2008 8.2.2.3**

<table>
<thead>
<tr>
<th>consequence (Asset value + C,I impact)</th>
<th>threat likelihood (considering VAN.5 level)</th>
<th>ease of vulnerability exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = no consequence on TOE dev</td>
<td>1 = low</td>
<td>1 = very hard (above VAN.5 level)</td>
</tr>
<tr>
<td>2 = med on TOE dev</td>
<td>2 = med</td>
<td>2 = hard (VAN.5 level)</td>
</tr>
<tr>
<td>3 = high on TOE dev</td>
<td>3 = high</td>
<td>3 = easy (under VAN.5 level)</td>
</tr>
</tbody>
</table>

- **Risk** = consequence * threat likelihood * ease of vulnerability exploitation

**Focus on risk acceptance criteria**

  ➤ **ISO/IEC 27001:2005 4.2.1 e) 4)**

In our case, threshold is: $2 \times 2 \times 2 = 8$ (take into account CC)

- risk acceptance criteria is **risk < 8**.
Example risk evaluation criteria (chosen by the risk “manager”)
- Level of risk is estimated
  ➔ ISO/IEC 27001:2005 4.2.1 e) 3)
  ➔ ISO/IEC 27005:2008 8.2.2.3

<table>
<thead>
<tr>
<th>consequence (Asset value + C,I impact)</th>
<th>threat likelihood (considering VAN.5 level)</th>
<th>ease of vulnerability exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = no consequence on TOE dev</td>
<td>1 = low</td>
<td>1 = very hard (above VAN.5 level)</td>
</tr>
<tr>
<td>2 = med on TOE dev</td>
<td>2 = med</td>
<td>2 = hard (VAN.5 level)</td>
</tr>
<tr>
<td>3 = high on TOE dev</td>
<td>3 = high</td>
<td>3 = easy (under VAN.5 level)</td>
</tr>
</tbody>
</table>

Risk = consequence * threat likelihood * ease of vulnerability exploitation

Focus on risk acceptance criteria
  ➔ ISO/IEC 27001:2005 4.2.1 e) 4)

In our case, threshold is: 2*2*2 = 8 (take into account CC)

 риск acceptance criteria is « risk < 8 ».
Risk treatment

- Four possibilities:

  - ISO/IEC 27001:2005 4.2.1 f)
    - Retention
      - In case that the risk level meets acceptance criteria
    - Reduction
      - Relevant Objectives/controls are selected in order to reduce the risk
    - Avoidance
      - Risks are avoided (laptops forbidden)
    - Transfer
      - Risks are transferred
Statement Of Applicability (SOA)

- For risk Reduction, a Statement Of Applicability is written
  - Control objectives and controls selected with a rationale
  - Control objectives and controls currently implemented
  - The exclusion and justification
Certified ISMS => PDCA
Certified ISMS => PDCA

Certification ensures that the ISMS is correctly established but also that the ISMS is correctly:
Certified ISMS => PDCA

Certification ensures that the ISMS is correctly established but also that the ISMS is correctly:

- Implemented
- Operated
- Monitored
- Reviewed
- Maintained & Improved
Certified ISMS => PDCA

Certification ensures that the ISMS is correctly established but also that the ISMS is correctly:
- Implemented
- Operated
- Monitored
- Reviewed
- Maintained & Improved
CC certification *gives* a security level for a product.

ISO 27001 certification *does not give* a security level for an ISMS.

But if the ISMS is “correctly established for CC”, ISO 27001 certification answers, for a part, to environment evaluation criteria. And therefore permit CC product certification.
CC certification **gives** a security level for a product.

ISO 27001 certification **does not give** a security level for an ISMS.

But if the ISMS is “correctly established for CC”, ISO 27001 certification answers, for a part, to environment evaluation criteria. And therefore permit CC product certification.

What do we mean by “correctly established for CC”?
ISMS perimeter vs. TOE environment development perimeter

TOE development environment scope.

Site 1
  Activity 1

Site 2
  Activity 2

Site 3
  Activity 5
  Activity 4

Activity 3

TOE
ISO/IEC 27001:2005 certified ISMS

ISMS perimeter vs. TOE environment development perimeter

Site 1
Activity 1

Site 2
Activity 2

Site 3
Activity 5
Activity 4

TOE

ISMS perimeter.

TOE development environment scope.
ISO/IEC 27001:2005 certified ISMS

ISMS perimeter vs. TOE environment development perimeter

Site 1
Activity 1
Site 2
Activity 2
Site 3
Activity 5
Activity 4
TOE

TOE development environment scope.
ISO/IEC 27001:2005 certified ISMS

ISMS perimeter vs. TOE environment development perimeter

Site 1
Activity 1

Site 2
Activity 2

Site 3
Activity 4
Activity 5

TOE

ISMS perimeter.

TOE development environment scope.
Method to check if the ISMS is correctly established “for CC”:

First
- The ISMS shall be certified

The evaluator checks the risk assessment/treatment part of the ISMS using the following 4 rules:
- Assets identified in the ISMS documentation are complete and consistent with the ST.
- Evaluation & acceptance criteria correctly takes into level of attacker and TOE development issues.
- Risks that do not meet acceptance criteria must be treated (management cannot change the risk acceptance criteria).
- Risks transfer option must be evaluated.

These checks can be performed during DVS/DEL work unit evaluation.
The evaluator does not check the SOA
- No procedure, security measure evaluation
The evaluator does not check the SOA
- No procedure, security measure evaluation

<table>
<thead>
<tr>
<th>ISMS evaluation</th>
<th>Security documentation evaluation</th>
<th>CM plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>10%</td>
<td>70%</td>
<td>20%</td>
</tr>
</tbody>
</table>
- The evaluator does not check the SOA
  - No procedure, security measure evaluation

<table>
<thead>
<tr>
<th>ISMS evaluation</th>
<th>Security documentation evaluation</th>
<th>CM plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>10%</td>
<td>70%</td>
<td>20%</td>
</tr>
</tbody>
</table>
The evaluator does not check the SOA
- No procedure, security measure evaluation
- Gain of workload and costs reducing (70%)
The evaluator does not check the SOA
- No procedure, security measure evaluation
- Gain of workload and costs reducing (70%)

No audit for DVS/DEL (covered by ISO certification)
The evaluator does not check the SOA
- No procedure, security measure evaluation
  → Gain of workload and costs reducing (70%)

- No audit for DVS/DEL (covered by ISO certification)
  - Audits are still to be performed for TOE related activities (CM, TAT)
The evaluator does not check the SOA
- No procedure, security measure evaluation
  ⇒ Gain of workload and costs reducing (70%)

No audit for DVS/DEL (covered by ISO certification)
- Audits are still to be performed for TOE related activities (CM, TAT)
  ⇒ Gain of workload and costs reducing (70%)
The evaluator does not check the SOA

- No procedure, security measure evaluation

→ Gain of workload and costs reducing (70%)

No audit for DVS/DEL (covered by ISO certification)

- Audits are still to be performed for TOE related activities (CM, TAT)

→ Gain of workload and costs reducing (70%)
The evaluator does not check the SOA
- No procedure, security measure evaluation
  ➞ Gain of workload and costs reducing (70%)

No audit for DVS/DEL (covered by ISO certification)
- Audits are still to be performed for TOE related activities (CM, TAT)
  ➞ Gain of workload and costs reducing (70%)
Advantages:
- ISMS and risk management are means for developer to be sure to succeed in DVS evaluation.
- ISMS and risk management give structured documentation easy to evaluate.
- ISO 27001 is recognized outside “CC world”.

Constraints:
- Costs induced by an 27001 certification
  - But this certification covers all products developed in the scope of the ISMS
Perform a pilot DVS/DEL evaluation
- Using the described method.

Extend this method to cover CM requirements
- By requiring “CM” controls (measures) for risk treatment.
Thank You!
Questions?