Executive Summary (v1)

Synopsis

This report presents the findings of an information security assessment according to the **"**STD Name" on the system Y Choose an item. by [Company]. The objectives of this work were to check the security and/or compliance level on the acceptance environment. This audit will especially aim to identify the vulnerabilities that can be used by an attacker to steal or manipulate information, or to disturb service, and thus degrade the reputation of [Company].

The audit has been performed from the XXnn to XXnn of MMMM YYYY in NNN facilities. According to itrust consulting’s methodology, **0** tests were planned and 0 points have effectively been tested (0 were out of scope and 0 were non-applicable).

According to the rules of evaluation applied to 0 domains included in the standard **"**STD" the evaluation is considered as Well implemented.

Results

After assessing the system according to "STD Name" (version V1.0) during Y days, itrust consulting concludes …

The audit established that the compliance level for the **0** considered domain(s) is Well implemented and to formulate the following non-compliance statements:

* major non-compliance(s) defined as a complete lack of documentation or implementation for one control point of the standard which lead to malfunctioning of the system.
* minor non-compliance(s) defined as a partial lack of documentation or implementation for one control point of the standard which do not lead to malfunctioning of the system.
* 0 remark(s) noticed a control point of the standard not correctly implemented according to security good practices or to improve by one or more precise actions.

The audit has also identified critical points that need to be reassessed and has formulated dedicated actions (corrective action, recommendations or mitigation measures):

* 0 actions, marked as , requiring an immediate implementation to avoid an inacceptable risk or a major nonconformity.
* 0 actions, marked as , requiring a prompt implementation to avoid a high risk or minor nonconformity.
* 0 actions, marked as , requiring a dedicated implementation to mitigate a medium risk.
* 0 suggestion(s), marked as , to improve the efficiency or the security of identified items which should be addressed in the normal improvement cycle.
* 0 hint(s) marked as 🗵, to (to be defined)
* 0 note(s) marked as 🗊, requiring specific assessment to ensure a correct evaluation or increase the assurance.

Executive Summary (v2)

Synopsis

This report presents the findings of an information security assessment according to the **"**STD Name" framework on the system Y Choose an item. by . The objectives of this work were to check the security and/or compliance level on the acceptance environment. This audit aims at finding or demonstrating vulnerabilities that can be used by an attacker to steal or manipulate information, or to disturb service, and thus degrade the reputation of .

The audit has been performed from the XXnn to XXnn of MMMM YYYY in NNN facilities. According to itrust consulting’s methodology, 0 tests were planned to be performed and 0 points have effectively been tested (0 were out of scope and 0 was/were non-applicable).

According to the rules of evaluation applicable for the 0 domains included in the standard "STD" the evaluation is considered as Well implemented.

Results

After assessing the system according to "STD Name" (version V1.0) during Y days, itrust consulting concludes …

The figures below provide in one hand a synthetic view of the recommendations identified during the audit and additional information provided to improve security and in the other hand an overview of the test performed with the relative classification used to assess the performance of the security measures implemented on the targeted system.

Figure 1: Summary view of recommendations and mitigation measures

Figure 2:Summary view of criterium results

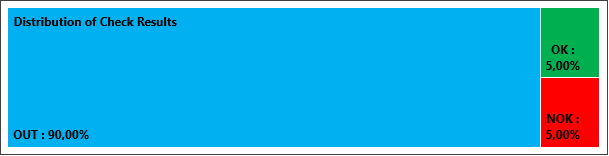


Figure 3: Distribution of check results for the overall criteria

Figure 4: Summary of findings related to

Details of the main results

Details of the security assessment

Main vulnerability

During the audit, itrust identified that most vulnerabilities concern the management of Infrastructure with 0 vulnerabilities.

Identified critical impact

Among the impacts [potential security breach] identified by itrust due to discovered vulnerabilities, the most important are:

| ID | Rating | [VUL] | Description |
| --- | --- | --- | --- |
| IMP. 1 | ▼▼▼▼ | [000] | Consequently to the vulnerability, the potential impact is… |

Immediate security action

In recommendation list:

Among the recommendations provided by itrust, the most important are:

| ID | Rating | Description |
| --- | --- | --- |
| REC. 2 |  | Do… (imperative tense). |
| REC. 4 |  | Do… (imperative tense) |

In mitigation list:

Among the mitigation measures provided by itrust, the most important are:

| ID | Rating | [VUL┆IMP] | Description |
| --- | --- | --- | --- |
| MIT. 2 |  | [000┆000] | Do… (imperative tense). |

In correction action list:

Among the corrective actions decided together with the customer, the list below summarizes the most important actions:

| ID | Rating | Deadline | Description |
| --- | --- | --- | --- |
| AC. 1 |  | 07/2014 | Do …(imperative tense) |
| AC. 2 |  | 07/2014 | Do… (imperative tense) |

Additional investigation

The following specific points need to be investigated in depth during an additional internal or external audit:

In recommendation list:

| ID | Rating | Description |
| --- | --- | --- |
| REC 12. |  | Do…(imperative tense) |

In correction action list:

| ID | Rating | Deadline | Description |
| --- | --- | --- | --- |
| AC 13. |  | 07/2014 | Do…(imperative tense) |

Positive points of customer implementation

During the audit, itrust has identified the following positive points regarding the robustness of security design or implementation of the system:

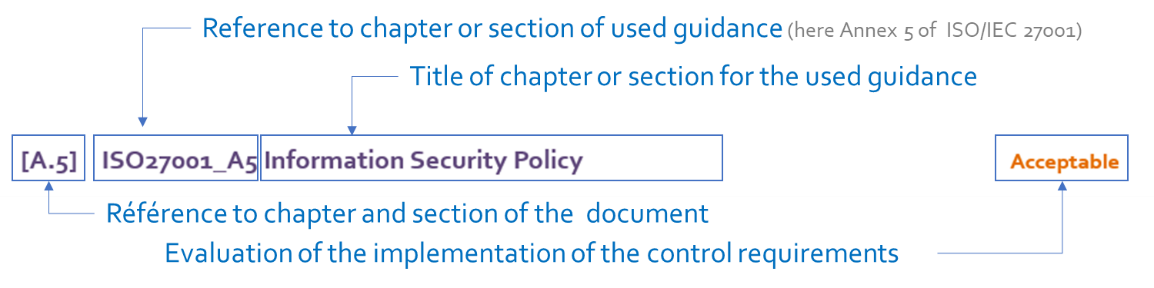
| ID | Rating | Description |
| --- | --- | --- |
| RP. 1 |  | The system presents…. (present tense) |
| RP. 2 |  | The system presents… (present tense) |

## Editorial convention used in the report

This chapter described the convention chosen for this report especially regarding the rating scale used to assess the security state of the targeted system and security actions which could be implemented to improve or maintain this level.

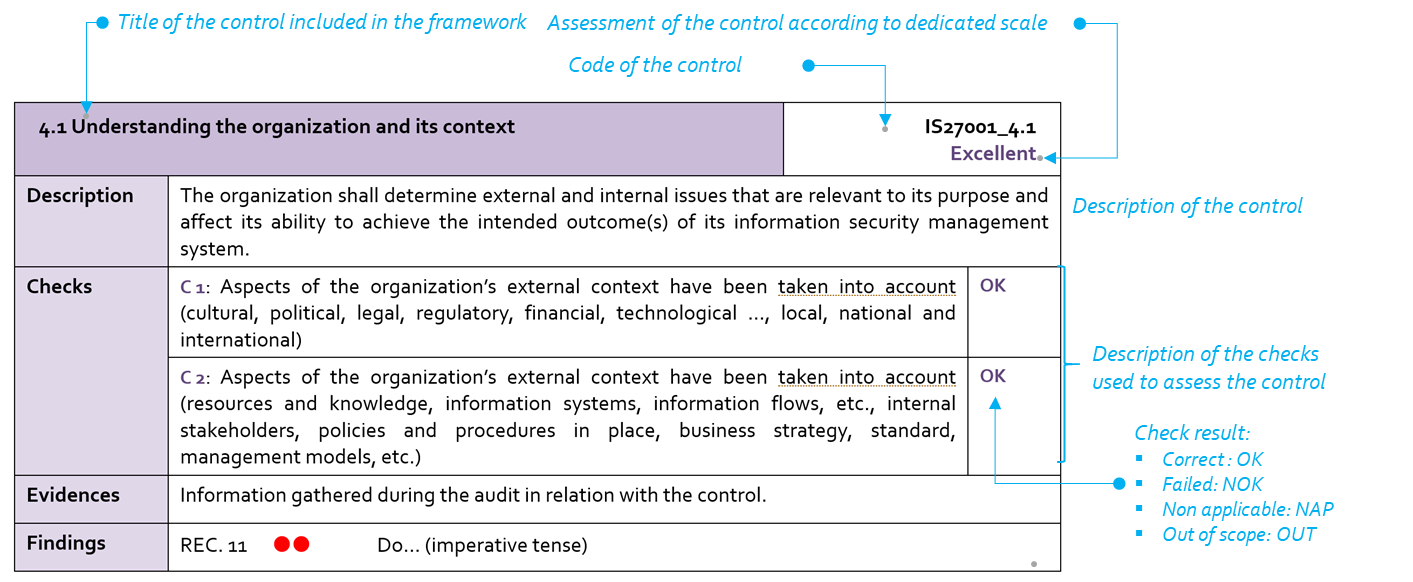
### Titling

To make reference to the standard or security guideline used during this audit, the present report adopts the following convention for the titling



### Description of the tables

The following example explains how to read the entire set of tables used in the present document.



Note: If audit items in one table refer to a more specific item in another table, the report will only assess that item once to avoid repeating the same non-conformity or corrective action within the document.

The assessment of the implementation of security good practices or of the targeted security controls will include both the evaluation of the conformity and maturity levels for the defined domain. The criteria to assess the implementation rate and the maturity level are described in the table below:

|  |  |  |
| --- | --- | --- |
| Maturity Level | CMMI Model | Description |
| Level 1 | Initial | Process / System unpredictable, poorly controlled and reactive. |
| Level 2 | Managed | Process / System implemented and managed by professionalism (proactive). |
| Level 3 | Defined | Process / System defined and implemented according to standardized approach. |
| Level 4 | Quantitatively Managed | Process / System regularly controlled and assessed. |
| Level 5 | Optimizing | Process / System regularly reviewed in a improvement cycle approach |

Table 1: Implementation and maturity criteria

### Report interpretation

The present report uses several scales to assess either compliance to security guidelines, criticality level of findings, security actions to implement, or general evaluation of tests performed during the review. The tables below describe the defined scales and give a short description of each level.

#### Definition of non-compliance level

The audit shall provide a compliance rating of the system according to "Name of the standard" standard and security good practices for each domain in order to provide a clear overview of the organisation’s level of security. The non-compliance of a domain is assessed as either major or minor. Remarks are provided to correct deficiency or to improve one point of the domain.

|  |  |
| --- | --- |
| Non-compliancy level | Description |
| Major Non-Compliance | A non-fulfilment of a requirement that affects the capability to achieve the intended results. Note Nonconformities could be classified as major in the following circumstances:   * if there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements; * a number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity. |
| Minor Non-Compliance | A non-fulfilment of a requirement does not affect the capability to achieve the intended results |
| Remark | An observation for consideration in the continuous improvement process or the risk treatment process. |

### Criteria/Vulnerability rating scale

The scale used to assess the result security criterion check is graduated into several levels of assessment:

|  |  |
| --- | --- |
| Scale | Description |
| Not rated | The auditor does not have sufficient evidence to conclude on this point. |
| Well implemented | The criteria are well met using measures that are beyond the state of the art and offer more security than standard implementations. |
| Appropriate | The criteria are correctly implemented in view of the state of the art. |
| Satisfactory | The criteria are implemented, but given the state of the art, the risks are under control, but areas for improvement have been identified. |
| To improve | The criteria are met at a minimum, but the overall safety of the system still presents acceptable but unnecessary risks, as consideration of the state of the art would have reduced them. |
| Partially satisfied | The criteria are generally met except for one or more specific elements that present limited risks. |
| Non satisfied | The criteria are by no means met: absence of necessary security measures constituting a clear vulnerability to the security of the systems. |
| Non tested | The criteria have not been checked on the target system. |
| Non applicable | The criteria are not applicable to the target system. |
| Out of scope | Control cannot be assessed due to the definition or nature of the target system. |

#### Domain rating scale

The scale used to assess a specific security domain is identical to that used to assess a security criterion or vulnerability (see above) but will cover all criteria or vulnerabilities related to that security domain.

#### Assessing the different security domains and the overall security

Although the evaluation of the various elements (control, security domain or general security of the target of evaluation) is left to the auditor's sole discretion, the auditor may also perform these evaluations automatically by applying the corresponding calculation matrices described below.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | A control is considered as | | | | | | |
|  | Not rated | Well implemented | Appropriate | Satisfactory | To improve | Partially satisfied | Non satisfied |
| First level of evaluation: if the sum of nonconformities and upper nonconformities is greater than or equal to: | | | | | | | |
| Major | Disenabled |  |  |  |  |  | 01 |
| Minor | Disenabled |  |  | 01 | 02 | 03 | 05 |
| Second level of evaluation: if the sum of recommendations for a level and upper levels is greater than or equal to: | | | | | | | |
|  | Disenabled |  |  |  |  |  | 001 |
|  | Disenabled |  |  |  | 001 | 002 | 005 |
|  | Disenabled |  |  | 001 | 002 | 005 | 010 |
|  | Disenabled |  | 002 | 003 | 005 | 010 | 020 |
| Third level of evaluation: if it includes a point rated at this level of robustness: | | | | | | | |
|  | Disenabled |  |  |  |  |  |  |
|  | Disenabled |  |  |  |  |  |  |
|  | Disenabled | 1 |  |  |  |  |  |
| Fourth level of evaluation: if the sum of specific points or additional controls is greater than or equal to: | | | | | | | |
| Add control  | Disenabled |  |  |  |  |  |  |
| Specific 🗵 | Disenabled | 001 |  |  |  | 015 | 020 |

Table 2: Assessment matrix for control

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | A domain is considered as | | | | | | |
|  | Well implemented | Appropriate | Satisfactory | To improve | Partially satisfied | Non satisfied |  |
| If the evaluation of the results of controls included in the relative domain and expressed in % by category,complies with the two sets of assessment rules: | | | | | | | |
| Not rated | Disenabled | Disenabled | Disenabled | Disenabled | Disenabled | Disenabled | 🡅≥  Rule 1 |
| Well implemented | 75 % | 0 % | 0 % | 0 % | 0 % | 0 % |
| Appropriate | 25 % | 75 % | 0 % | 0 % | 0 % | 0 % |
| Satisfactory | 0 % | 25 % | 75 % | 0 % | 0 % | 0 % |
| To improve | 0 % | 0 % | 25 % | 75 % | 0 % | 0 % |
| Partially satisfied | 0 % | 0 % | 0 % | 25 % | 75 % | 25 % | 🡇≤  Rule 2 |
| Non satisfied | 0 % | 0 % | 0 % | 0 % | 25 % | 75 % |

Table 3: Assessment matrix for domain

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | The overall security of the targeted system is considered as | | | | | | |
|  | Well implemented | Appropriate | Satisfactory | To improve | Partially satisfied | Non satisfied |  |
| If the evaluation of the results of the overall domains expressed in % by categories complies with the two sets of assessment rules: | | | | | | | |
| Well implemented | 75 % | 0 % | 0 % | 0 % | 0 % | 0 % | 🡅≥  Rule 1 |
| Appropriate | 25 % | 75 % | 0 % | 0 % | 0 % | 0 % |
| Satisfactory | 0 % | 25 % | 75 % | 0 % | 0 % | 0 % |
| To improve | 0 % | 0 % | 25 % | 75 % | 0 % | 0 % |
| Partially satisfied | 0 % | 0 % | 0 % | 25 % | 75 % | 10 % | 🡇≤  Rule 2 |
| Non satisfied | 0 % | 0 % | 0 % | 0 % | 25 % | 90 % |

Table 4: Assessment matrix for the overall system

#### Criticality scale of provided security actions

The table below describes the scale of criticality used to evaluate the level of security actions (recommendations or correctives actions) provided in the audit report:

|  |  |  |
| --- | --- | --- |
| Rating | Tag | Description |
|  | Critical | A situation of unacceptable risk or major non-compliance that requires immediate action (typically on the day of discovery). |
|  | Urgent | A situation of risk or non-compliance that is unacceptable from a security, contractual or legal point of view, but which could be temporarily accepted by management based on other considerations beyond the scope of the present assessment. |
|  | Important | Acceptable but unnecessary risk situation or lack of recommended state of the art measures. |
|  | Useful | A situation of low risk or lack of effectiveness, with known suggestions for improvement. |
|  | Specific | Optional type of recommendation (to specify) |
|  | To be checked | Need for more specific investigations than those provided for in this project. |

#### Robustness scale

If controls or tests show the security of the system is above the average of security good practices, the auditor could use the following scale to stress on this security robustness of the system:

|  |  |
| --- | --- |
| Rating | Description |
|  | The security measure is based on an innovative and sustainable solution ensuring a real security in depth. |
|  | The security measure is based on the most secure known solution. |
|  | The security measure chosen is adequately above the average security solution used in similar cases. |

#### Vulnerability model

The vulnerabilities identified on the targeted system are sorted using the following vulnerability model:

|  |  |  |
| --- | --- | --- |
| Symbol | Name | Description |
| **🏭** | Infrastructure | Vulnerable security system of the infrastructure such as fire protection system, cable redundancy, power supply, etc. |
| **🖧** | Network | Vulnerability of the network and relative equipment such as switch, firewall, router, etc. |
| **💻** | Hardware | Vulnerability of implemented hardware such as dimensioning error for the chosen equipment, unsecured equipment, etc. |
| **🗗** | Software | Vulnerability of software generally known according to software vulnerabilities database. |
| **🛠** | Deployment | Vulnerability due to default of implementation, configuration or maintenance. |
| **👁** | Management | Vulnerability on the security management: lack of qualified personnel, lack of work time for security management. |
| **🚹** | Human | Direct or indirect vulnerability relative to personnel implementing the system such as lack of awareness. |

#### Impact scale

According to the vulnerabilities discovered, the present report establishes the potential impact for the targeted system in case of vulnerability exploitation. The following scale of impact is used to assess the criticality of the impact:

|  |  |  |
| --- | --- | --- |
| Symbol | Name | Description |
| **▼▼▼▼** | Critical | The system or process supported by the vulnerable asset is:  totally destroyed *— e.g. destruction of equipment due to fire.*  inoperable during a long time *— e.g. malicious encryption of a hard-drive.* |
| **▼▼▼** | High | The system or process supported by the vulnerable asset is compromised (loss of control, confidentiality or integrity properties). *— e.g. installation of a Remote Access Terminal* |
| **▼▼** | Medium | The behavior of the system or process supported by the vulnerable asset is altered by the attack but without loss of control or loss of confidentiality and integrity properties.  *— e.g. speed reduction of computing processes.* |
| **▼** | Low | The system or process supported by the vulnerable asset still remains operational, but the security shielding became ineffective and increases the vulnerability of the entire system.  *— e.g. bad configuration of a firewall.* |

This line include an essential bookmark E\_F: do not remove

# Conclusion

After X days of audit on the targeted system, itrust concludes that Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum

The tables below give a clear summary of findings, tests performed and security levels of the system according to the customer’s needs in terms of scope, depth and granularity of the audit.

## Assessment of security domains

The table below gives a summary of the assessment of the domains considered during the audit and also the final evaluation of the compliance.

|  |  |  |
| --- | --- | --- |
| Evaluation of the considered domains | | Total/Type |
| Well implemented | | 0 |
| Appropriate | | 0 |
| Satisfactory | | 0 |
| To improve | | 0 |
| Partially satisfied | | 0 |
| Non satisfied | | 0 |
| Non applicable | | 0 |
| Out of scope | | 0 |
| Global result | Partially satisfied | |

Table 5: Global result of security domains assessment for the targeted system

In conclusion, the audit of ’s system has been evaluated according to **0** of **0** domains included in the standard … and is considered asPartially satisfied.

Detailed Rating[[1]](#footnote-1)

| Reference | Title | Rating |
| --- | --- | --- |
| [\*.\*] | Acronym and title of domain | Rating |

Table 6: Results per security domain

## Assessment of the non-compliances

The conclusion of the audit performed on the target has led itrust to identify non-compliance and provide feedback on the implementation.

The tables below give a synthesized overview of the non-compliances and formal remarks included in this document.

|  |  |
| --- | --- |
| Non-compliance | Total/Type |
| Major complete lack of documentation or implementation | 1 |
| Minor partial lack of documentation or implementation | 0 |
| Remarks point to be corrected or improved | 0 |
| Total | 1 |

Table 7: Summary of non-compliance points

The list below provides the details of the recommendations resulting from security review on the target:

| ID | Rating | Ref. | Description |
| --- | --- | --- | --- |
| NC1. | Minor | 9.9.9 |  |

Table 8: List of non-conformities

## Summary of identified vulnerabilities

The table below gives an overview of vulnerabilities identified during the audit according to their type.

|  |  |
| --- | --- |
| Type of vulnerability | Total/Type |
| 🏭 Infrastructure | 0 |
| 🖧 Network | 1 |
| 💻 Hardware | 0 |
| 🗗 Software | 0 |
| 🛠 Deployment | 0 |
| 👁 Management | 0 |
| 🚹 Human | 0 |
| Total | 1 |

Table 9: Summary of identified vulnerabilities

The list below provides the details of the vulnerabilities discovered during the security review performed on the system deployed by :

| ID | Type | Description |
| --- | --- | --- |
| VUL 1. |  | The system presents the following vulnerability |

Table 10: List of vulnerabilities per type

## Summary of potential impact

In parallel with the assessment of the vulnerabilities, the audit provides the potential impact in case of vulnerability exploitation by their criticality level.

|  |  |
| --- | --- |
| Impact level | Total/Type |
| ▼▼▼▼ Critical | 2 |
| ▼▼▼ High | 0 |
| ▼▼ Medium | 0 |
| ▼ Low | 0 |
| Total | 2 |

Table 11: Summary of potential impacts

The list below provides details of the potential impact in case of vulnerability exploitation:

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Level | Vul. | Description |
| IMP.1 | ▼▼▼▼ | [001] | Consequently to the vulnerability, the potential impact is… |

Table 12: List of potential impacts

## Summary of identified correctives actions

Below gives a summary of the identified corrective actions agreed with the customer to ensure or increase the security level of the tested system and to restore compliance if necessary.

|  |  |
| --- | --- |
| Corrective action level | Total/Type |
|  Immediate action required | 1 |
|  Prompt action required | 2 |
|  Dedicated action required | 0 |
|  Hints useful for improving security | 0 |
| 🗵 Not defined | 0 |
| 🗊 Additional investigation/control required | 0 |
| Total | 3 |

Table 13: Summary of identified corrective actions

The list below provides the details of the corrective actions resulting from the security review performed on the system deployed by :

| Ref. | Rating | Deadline | Description |
| --- | --- | --- | --- |
| AC. 1 |  | 07/2014 | Do... (Imperative tense) |

Table 14: List of corrective actions

## Summary of identified recommendations

The table below gives a synthesized overview of the identified recommendations to ensure or increase the security level of the system and to restore compliance if necessary:

|  |  |
| --- | --- |
| Recommendation level | Total/Type |
|  Immediate action required | 2 |
|  Prompt action required | 1 |
|  Dedicated action required | 1 |
|  Hints useful for improving security | 0 |
| 🗵 Not defined | 0 |
| 🗊 Additional investigation/control required | 0 |
| Total | 4 |

Table 15: Summary of identified recommendations

The list below provides the details of the recommendations resulting from the security review on the system deployed by :

| Ref. | Rating | Description |
| --- | --- | --- |
| REC. 1 |  | Do... (imperative tense) |

Table 16: List of recommendations

## Robustness of customer implementation

During the audit, the auditor has identified positive points in the design, implementation and maintenance of the targeted system. Among these positive points, the following points can be considered as the basis of the system’s robustness:

| ID | Rating |  |
| --- | --- | --- |
| RP. 1 |  | The system presents… |

Table 17: List of identified robustness points

## Summary of the results per security criterium

The table below gives an overview of the results per criterium according to a defined scale (included previously in the document):

|  |  |
| --- | --- |
| Criterium assessment results | Total/Type |
| Not rated | 0 |
| Well implemented | 2 |
| Appropriate | 0 |
| Satisfactory | 1 |
| To improve | 20 |
| Partially satisfied | 1 |
| Non satisfied | 2 |
| Non tested | 0 |
| Non applicable | 0 |
| Out of scope | 0 |
| Total | 26 |

Table 18: Summary of criterium results

The table below gives the details of the tests performed with their rating.

| Reference | Title | Rating |
| --- | --- | --- |
| REF9999\_0.0.0 | 0. Editorial Convention | To improve |

Table 19: List of results per security criterium

## Summary of the check results per criterium and domain.

The table below gives an overview of the results per criterium according to a defined scale (included previously in the document):

|  |  |
| --- | --- |
| Checks assessment results | Total/Type |
| OK (Checks satisfied) | **3** |
| NOK (Checks not satisfied) | 3 |
| OUT (Checks out of scope) | **5** |
| NAP (Checks not applicable) | 4 |
| Total |  |

Table 20: Summary of checks results

The table below provides an overview of the overall results of the checks carried out for each control.

| Reference | Title | OK | NOK | OUT | NAP | Rating |
| --- | --- | --- | --- | --- | --- | --- |
| [2] | First domain XXXX | 1 | 2 | 3 |  | Partially satisfied |

Table 21: Distribution of check results per criterium and domain

## Summary of identified mitigation measures

The table below gives an overview of mitigation measures identified during the audit according to their criticality.

|  |  |
| --- | --- |
| Criticality level of mitigation | Total/Type |
|  Immediate action required | **1** |
|  Prompt action required | **1** |
|  Dedicated action required | **0** |
|  Hints useful for improving security | **0** |
| Total | 2 |

Table 22: Summary of identified mitigation measures

The table below list the security measures identified to mitigate vulnerabilities on the targeted system:

|  |  |  |  |
| --- | --- | --- | --- |
| Ref | Level | [VUL┆IMP] | Description |
| MIT. 1 |  | [000┆000] | To mitigate the identified vulnerability and avoid impact, do ... (imperative tense) |

Table 23: List of mitigation measures

## Summary of findings related to

The table below gives an overview of the findings related to established during the audit according to the defined scale:

|  |  |  |
| --- | --- | --- |
| Summary by type of results | | Total/Type |
|  | Description of the level |  |
| Total | |  |

Table 24: List of findings related to

The table below list the findings related to identified during the audit:

|  |  |  |
| --- | --- | --- |
| Ref | Level | Description |
| CUST. 1 |  | Description of the customized findings |

Table 25: List of findings related to

## Global security assessment of the tested system

The table (security panel) below give a synthesis panel of the security level for the tested system according to the vulnerability assessment. Additionally it provides the list of recommendations identified according to the potential impact of an attack targeting a specific vulnerability.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID VUL | Type | Description of Vulnerability | ID IMP | Level | Description of Impact | ID MIT | Level | Description of recommendation |
| 001 |  | Description of vulnerability | **001** | ▼▼▼▼ | Potential Impact if exploitation | **001** |  | Mitigation measure |

Table 26: Security panel

This line includes an essential bookmark C13: do not remove

1. The number of chapter into bracket shows that the evaluation has been focused on a specific sub-domain of the standard in order to check specific and mandatory points. [↑](#footnote-ref-1)