Data Cybersecurity Evaluation with ISO/IEC 25012

Javier Verdugo [1], Moisés Rodríguez [2], Jesús Oviedo [3], Mario Piattini [4]

[1,2,3,4]AQCLab, Instituto de Tecnologías y Sistemas de Información, Cam. Moledores s/n, 13005, Ciudad Real, Spain
[4] Alarcos Research Group - UCLM, Escuela Superior de Informática, Paseo de la Universidad 4, 13071, Ciudad Real, Spain

Abstract

As arguably one of the most valuable assets for many companies, if not the most, data quality and, specifically, data security have been drawing growing attention from the perspective of standards -being the ISO/IEC 27000 series the most prominent- and regulations -such as the GDPR and the Cybersecurity Act. Nonetheless, they are focused on security management systems and infrastructure, rather than in the intrinsic security aspects that can be attributed to the data itself. Other standards such as ISO 8000, which focuses on data quality, also pay little attention to data security. In this paper the authors propose a framework for the evaluation of data cybersecurity, taking the ISO/IEC 25000 series as a basis for the quality model and evaluation process that have been defined. The evaluation framework proposed has been validated in a pilot project with a commercial product, and currently is under further validation as it is intended to be the foundation for a data cybersecurity certification scheme defined in collaboration with the leading certification body in Spain.

Keywords

Data cybersecurity, data quality, data evaluation, data certification, ISO/IEC 25012

1. Introduction

The growing importance of data as a driver of business value has led to an increase in the attention paid to data quality and, specifically, security. This increasing awareness has not only been raised by private organizations, but also by regulation authorities. An example of this is the Cybersecurity Act reached by the European Parliament, the Council and the European Commission, which introduces an EU-wide cybersecurity certification framework for ICT products, services and processes [1]. Another example is the General Data Protection Regulation (GDPR) [2], also enacted by the European Parliament and the Council of the European Union, which aims at protecting natural persons with regard to the processing of personal data and the free movement of such data.

Even if the GDPR defines a specific section for the security of personal data (establishing the obligation to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk), and the Cybersecurity Act aims at certifying ICT products, their main focus is set on infrastructure and management systems, but not on the security of the data itself.

The authors of this paper have implemented an evaluation framework which focuses on data security itself. This framework consists of a quality model, an evaluation process, and a technological environment. They are currently collaborating with AENOR (the leading certification body in Spain) to use the evaluation framework defined as the foundation for a data cybersecurity certification. This certification is to be included in AENOR's Cybersecurity and Privacy scheme, which currently includes several

4th International Workshop on Experience with SQuaRE series and its Future Direction, December 06, 2022, Tokyo, Japan
EMAIL: jverdugo@aqclab.es (A. 1); mrodriguez@aqclab.es (A. 2); joviedo@aqclab.es (A. 3); mpiattini@uclm.es (A. 4)
ORCID: 0000-0002-2526-2918 (A. 1); 0000-0003-2155-7409 (A. 2); 0000-0001-7962-1042 (A. 3); 0000-0002-7212-8279 (A. 4)

standards from the ISO/IEC 27000 series and the eIDAS UE regulation.

2. Data Cybersecurity Evaluation Model

The data cybersecurity evaluation model proposed has been included as part of the evaluation framework of AQCLab, an accredited laboratory for which the authors work, and which performs software product Functional Suitability [3], software product Maintainability [4] and Data Quality [5] evaluations, all of them based on the ISO/IEC 25000 series of standards.

As Figure 1 shows, the data cybersecurity model follows a hierarchical approach with four different levels. The topmost level corresponds to the Data Cybersecurity itself as the attribute that encompasses all the other elements in the model. On the following level, the model defines a set of quality characteristics, which have been selected from the ISO/IEC 25012 standard [6]. The third level establishes a set of quality properties, which have been adapted from ISO/IEC 25024 [7]. Finally, the fourth level corresponds to the base measures that are obtained from the evaluated data repository and the information system to which it belongs.

An evaluation provides as a result a value for data cybersecurity in the range of 1 to 5. This value represents a quality level that goes from deficient cybersecurity for the lowest level to excellent cybersecurity for the highest one. This value is obtained as an aggregation of the values of the attributes in the second level (quality characteristics).

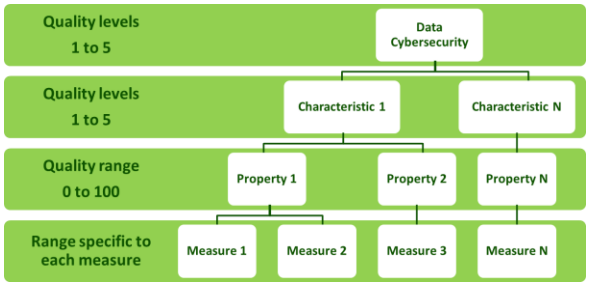

Figure 1: Hierarchical approach for the Data Cybersecurity model

2.1. Quality Characteristics

The five characteristics from ISO/IEC 25012 selected for the data cybersecurity model because of their close relation to security aspects are the following:

- **Compliance**: degree to which data adhere to standards, conventions, regulations, and similar rules relating to data quality.
- **Confidentiality**: degree to which data are ensured to be accessible and interpretable only by authorized users.
- **Traceability**: degree to which an audit trail is provided regarding access and changes made to the data.
- **Availability**: degree to which data can be retrieved by authorized users and/or applications.
- **Recoverability**: degree to which data maintain and preserve a specified level of operations and quality, even in the event of failure.

The characteristics in the model, in a similar way to the overall value for data cybersecurity, take a value in the range1 to 5 as a result for their evaluation.

2.2. Quality Properties

Quality properties are the basis for the evaluation of quality characteristics. Quality properties focus on specific concerns that affect a quality characteristic.

The quality properties selected for the data cybersecurity model, shown in Table 1, have been adapted from the quality measures proposed in ISO/IEC 25024.

Quality properties take a quality value in the range 0 to 100. This value is obtained by using an evaluation function that is defined in a standard way in the model, and which is specific to each of them. This evaluation function is applied over a set of base measures which are calculated over different target entities in the data repository or the information system to which it belongs. The target entities have quantifiable attributes that are measured to provide the base measure values. Some examples of target entities for the properties in the model are data files (tables), elements of data architecture (contextual schema, data models, data dictionary) and elements of system architecture (database management system, documents, forms, presentation devices).

Table 2 provides an example of the information that the model defines for each quality property shown in Table 1. In this case, the property represented in the example is Regulatory compliance of value and/or format.

Table 1
Quality properties in the data cybersecurity evaluation model

Characteristic	Properties
Compliance	Regulatory compliance of value and/or format
	Regulatory compliance due to technology
Confidentiality	Encryption usage
	Non-vulnerability
Traceability	Users access traceability
	Data values traceability
Availability	Probability of data available
	Architecture elements availability
Recoverability	Data recoverability ratio
	Periodical backup
	Architecture recoverability

Besides the general information for each quality property, the model also defines how to obtain the value for their corresponding base measures. Table 3 continues the example shown in Table 2 by providing detail on the base measures for the property Regulatory compliance of value and/or format.

Table 2
General information for the property Regulatory Compliance of Value and/or Format

Property	Regulatory compliance of value and/or format
Characteristic	Compliance
Description	Degree to which data values and/or format comply with specific standards, conventions, or regulations. The organization is responsible for identifying or establishing the rules to which the data must comply in terms of value and/or format. These rules can be established either internally, by the organization, or by external regulatory bodies.
Point of view	Inherent
Evaluation Function	Profiling function

For this property, as for others in the model, the measurement is dependent on specific business rules that the data in the repository (or other elements in the information system) must comply to. These rules can be set by national or local regulations, by regulators of the sector in which the company operates, internally by the own company, etc.

The base measure shown in Table 3 is measured for each file in the data repository. Then, as Table 2 indicates, a profiling function is used to derive the property value from the base measurements. This profiling function first obtains the profile for the data repository, which is the percentage of the data files categorized in each of the profile ranges shown in Table 4. Then, a quality value is calculated from that profile.

Table 3
Measurement information for the property Regulatory Compliance of Value and/or Format

Target entity	Data file (table)
Target attribute	Data record(row)
Measurement description	Regulatory compliance of value and/or format for a data file is obtained as the ratio of records of that file whose value for their fields comply with specific rules, conventions or regulations that have been established.
Calculation formula	X=A/B X= regulatory compliance of value and/or format for data file A= number of records that have values and/or format that conform to standards, conventions, or regulations B= number of records that shall conform to standards, conventions or regulations owing to their value
Scale	Ratio
Value range	[0.0 - 1.0]

3. Evaluation Process

The evaluation process defined in the framework has been adapted from the process established by ISO/IEC 25040 [8]. However,

there are some nuances in the process that has been defined with respect to the standard.

Table 4
Profile ranges for the evaluation of Regulatory Compliance of Value and/or Format

Range	Description
[0.0 – 0.6)	Low regulatory compliance of value and/or format
[0.6 – 0.75)	Medium regulatory compliance of value and/or format
[0.75 – 0.95)	High regulatory compliance of value and/or format
[0.95 – 1.0]	Very high regulatory compliance of value and/or format

ISO/IEC 25040 defines a process that can be followed in any quality evaluation, considering that each of them may have their own objective. However, this is not the case for the Data Cybersecurity evaluations carried out by AQCLab, since its objective and the evaluation framework that is used remains the same for every evaluation performed. This means that, as regards the first activity of the process (Establish the requirements of the evaluation), it is not required in each evaluation to carry out tasks for defining its stringency. The other tasks established in the standard for this activity need to be performed in every evaluation, since it is necessary to establish its purpose (although it does not have an effect in the way in which the evaluation framework is applied), establish its requirements (which characteristics of the model will be evaluated, which rules apply to the system/repository) and identify the specific elements to be included in the scope of the evaluation.

In the same way, for the second activity of the process (Specify the evaluation) the tasks regarding selecting quality metrics and defining decision criteria for the quality measures and the evaluation are not necessary, since they are already predefined as part of the evaluation framework. Nonetheless is necessary to match the rules applying to the system/repository to the corresponding properties and base measures and deciding how they will be checked (tools to be used) depending on the technologies used in the implementation of the system/repository.

The other three activities proposed by ISO/IEC 25040 (Design the evaluation, Execute the evaluation, and Conclude the evaluation) are carried out in every evaluation with no adaptations as regards the tasks established in the standard.

4. Technological Environment

The framework defined relies on a technological environment to carry out the evaluations. Such an environment is necessary to perform evaluations in a practical, efficient, and accurate manner. This technological environment consists of tools that automate the acquisition, calculation and presentation of the values obtained for the different attributes in the quality model (base measures, properties, characteristics, and the overall data cybersecurity value). Three different tools (or type of tools) are considered for this purpose: measurement tools, an evaluation tool and a visualization tool.

Since the base measures of the model are observed directly on different elements (or target entities) of the information system or data repository to be evaluated, the measurement tools used in each evaluation for that purpose depend vastly on their specific technologies. For example, in the case of relational databases, a query tool is typically used to perform the require checks against the DBMS and obtain the information required for certain measures of the model.

Besides the specific tools required for the base measures, AQCLab has implemented an evaluation tool that applies the decision criteria of the evaluation model. This process is carried out automatically by the tool, taking the values for the base measures as input and applying the corresponding evaluation functions that represent the decision criteria defined in the model as thresholds and profiles. To determine the quality value for each attribute in the model, a bottom-up approach is followed, starting with the properties and scaling up in the model to get values for the characteristics and finally the overall data cybersecurity value. The values calculated by the evaluation tool are stored in a database, so that they can be later checked.

To check the evaluation results in a clear and easy way, a visualization tool has been developed. This tool can be used by both evaluators and clients. When the user selects an evaluation (from among those available depending on his/her role), the information is displayed by means of tables and graphics (radar charts and bar charts) with coded colors which help to interpret the results in

a visual way. This visualization tool also provides some added value functionalities, such as generating downloadable reports for evaluations or checking trends for repositories that have been evaluated at several points in time.

5. Pilot Project

The evaluation framework has been applied to an existing commercial product to validate it and verify the feasibility of performing evaluations with this framework. This pilot project was carried out with the intention of identifying possible drawbacks regarding the properties and measures selected for the model and their applicability to real-life information systems and data repositories, as well as, in general, to identify possible improvements to the framework.

The product evaluated in this pilot project was a business dashboard management tool based in the balanced scorecard (BSC) approach. Following a SaaS model, this tool allows its users to define, monitor and control KPIs with a visual dashboard. The information contained in the data repository of this tool corresponded to users' accounts, permissions, KPI definitions and classifications, measurements for the KPIs, configuration and preferences and system logs.

The pilot project involved two iterations of the evaluation process: the first one to get the data cybersecurity results of the system and repository as it was implemented and used in that moment, and the second one after the company responsible for the evaluated system made some changes and improvements (both to the system and the data) to address the shortcomings detected in the first evaluation.

5.1. First Iteration of the Evaluation

During the first activity of the process of the first iteration (*Establish the evaluation requirements*), the client identified the data repository and elements of the information to be included in the scope of the evaluation. The specific requirements for certain characteristics were elicited from the client, such as business rules regarding value or format for some data fields, fields that must contain encrypted data with a specific algorithm, the frequency of the backups, etc.

As part of the activity *specify the evaluation*, the elicited rules were mapped to the properties of the model they were related to. Afterwards, the *design of the evaluation* was carried out, elaborating the evaluation plan.

The *execution of the evaluation* started by performing the base measurements on the target entities according to their specification in the model and the specific rules identified with the client. Once the base measures were obtained, the evaluation tool was used to automatically calculate the values for properties, characteristics, and the overall data cybersecurity result. The quality values obtained in this first iteration of the evaluation for the characteristics and the data cybersecurity are shown in Table 5. The value for the overall data cibersecurity is obtained by applying a profiling function over the values for the characteristics.

Table 5
Quality values obtained in the first iteration of the evaluation

Characteristic	Value
Compliance	4
Confidentiality	2
Traceability	2
Availability	5
Recoverability	2
Data Cibersecurity	2

To *conclude the first iteration of the evaluation*, a report was generated and then provided to and reviewed with the client organization. Some of the shortcomings that led to these results are the following:

- The value for Compliance was impacted by some requirements regarding value and format of the data not being fully met. For example, that was the case for the rule about usernames and email addresses for user accounts not being duplicated.
- Penetration testing had not been performed, leading the property Non-vulnerability to obtain a quality value of 0. This in turn had a significant impact in the value for Confidentiality.
- The value for Traceability was impacted by some requirements regarding the property Data values traceability not being met. There was a rule established by the client that for the entities perspectives and objectives a log of changes made by the users should be maintained, but that information was not actually being recorded in the corresponding tables of the database.

- The value for Recoverability was low because there were some issues with the properties Periodical Backup and Architecture Recoverability. As regards Periodical Backup, the frequency of the backups resulted in a significant desynchronization between the information backed up for several tables and their content in the production environment right before the next scheduled backup execution. As for Architecture Recoverability, the elements of the architecture identified for the product were not being backed up.

The shortcomings detected were analyzed in order to identify improvement actions over the data in the repository, which were addressed before starting the second iteration of the evaluation. Nonetheless, some of the improvement actions required could not be actioned by the client before the second evaluation. For example, the client could not implement penetration testing because of they lacked experience in this matter and the costs of externalizing the service were not viable for them at that moment.

5.2. First Iteration of the Evaluation

After the client implemented the chosen improvement actions identified after the first iteration, a second iteration of the evaluation was performed. This second iteration had the goal of assessing how the improvements implemented might have an impact and thus be reflected in the results of the evaluation.

The process carried out in the second iteration was similar to the one in the first iteration, although some of the tasks and steps taken in the latter were not necessary in the second iteration. For example, when *establishing and specifying the evaluation*, it was not necessary to identify business rules nor update their mapping to properties, since there were not changes in that regard. On the other hand, the elements in the scope changed since improvements were implemented on them; then, the updated versions of these elements were provided by the client.

After the evaluation plan for the second iteration was prepared, the *evaluation was executed*. This way, the values for the base measures were obtained taking the updated elements as input. Then, parting from these base measures, the values for the properties, characteristics and overall Data Cybersecurity were obtained with the evaluation tool. The results for this second iteration of the evaluation are shown in Table 6. The results obtained show that the improvements made by the client were indeed reflected in the higher quality values for some characteristics and the overall Data Cybersecurity value. These results show that incorporating improvements regarding the security of the data and mitigating the risk associated with it leads to a corresponding better result when applying the evaluation framework.

To *conclude the evaluation*, a new evaluation report was generated and reviewed with the client, and the elements provided for the evaluation were eliminated from the laboratory systems.

Table 6
Quality values obtained in the second iteration of the evaluation

Characteristic	Value
Compliance	5
Confidentiality	2
Traceability	3
Availability	5
Recoverability	4
Data Cibersecurity	3

5.3. Analysis of the Pilot Project

This pilot project allowed us to verify that the framework defined, based on standards of the ISO/IEC 25000 series, can be used to evaluate different aspects of data cybersecurity.

The results obtained in the two evaluation iterations that were performed show that the evaluation model is sensitive to changes in aspects related to data cybersecurity, with the values in the second evaluation reflecting the improvements that were made to the repository after the first iteration.

6. Certification

As the laboratory AQCLab has done previously with other evaluations, such as the ones regarding Software Functional Suitability, Software Maintainability or Data quality mentioned in Section I, the objective is that, based on the evaluation of the cybersecurity of the data of a data repository, it can obtain a certification

issued by an accredited entity for this purpose if an adequate level of quality is achieved.

For this matter, AQCLab has contacted AENOR, the leading certification body in Spain, with the objective of including the certification of Data Cybersecurity within its Digital Ecosystem, and both parties are currently collaborating to materialize it.

This ecosystem from AENOR includes a Cybersecurity and Privacy scheme which offers solutions to the new cyber risks and threats faced by public and private organizations when facing their digital transformation. Currently it comprises certifications of compliance to several standards in the ISO/IEC 27000 series (ISO/IEC 27001, ISO/IEC 27032, ISO 27017 and ISO 27018), compliance to the eIDAS-PSC UE 910/2014 regulation, and compliance to the Spanish ENS (Esquema Nacional de Seguridad - National Security Scheme).

The certification process that is being defined with AENOR works in the following way: once the data cybersecurity evaluation of a system/repository has been completed by the laboratory, if the results of the evaluation show that an adequate level of quality has been achieved for the characteristics of the cybersecurity model (this means achieving level 3 or above), the client organization may opt for its certification. AENOR would then take the evaluation report as a basis to the issuance of the certificate.

7. Conclusion

This work presents a framework for data cybersecurity evaluation based on international standards, consisting of a quality model, an evaluation process, and a technological environment.

A pilot project has been conducted to validate that the proposed framework can be used to evaluate the cybersecurity of the data that companies manage and work with as part of their business mission. In the future, we intend to carry out more evaluations with this framework to obtain more practical knowledge about its application and identify further improvements.

Currently, AQCLab is collaborating with the leading certification body in Spain to use the results of the data cybersecurity evaluations carried out by the laboratory as a basis for a certification scheme.

8. Acknowledgements

Funded by Junta de Comunidades de Castilla-La Mancha through the project Q2SM: Quality Quantum Software Model (13/22/IN/032) and by the Spanish Ministry of Science and Innovation (MICINN) and EU through the projects QSERV: Quantum Service Engineering: Development Quality, Testing & Security of Quantum Microservices (PID2021-124054OB-C32) and AETHER: Una Aproximación holística de Smart data para el análisis de datos guiado por el contexto centrada en la calidad y la seguridad (PID2020-112540RB-C42).

9. References

[1] European Comission website, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[2] European Union Law website, https://eur-lex.europa.eu/eli/reg/2016/679/oj

[3] Rodríguez, M., Oviedo, J. R., Piattini, M.: Evaluation of software product functional suitability: a case study. Software Quality Professional 18 (3), 18-29, 2016.

[4] Rodríguez, M., Piattini, M., Fernandez, C. M.:A hard look at software quality: pilot program uses ISO/IEC 25000 family to evaluate, improve and certify software products. Quality Progress 48, 30-36, 2015.

[5] Gualo, F. Rodriguez, M., Verdugo, J., Caballero, I., Piattini, M.: Data quality certification using ISO/IEC 25012: industrial experiences. Journal of Systems and Software 176, 2021

[6] ISO/IEC 25012:2008 Software Engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Data Quality Model. International Organization for Standardization / ISO/IEC JTC 1/SC 7 Software and systems engineering, 2008.

[7] ISO/IEC 25024:2015 Software Engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Measurement of data quality. International Organization for Standardization / ISO/IEC JTC 1/SC 7 Software and systems engineering, 2015.

[8] ISO/IEC 25040:2011 Software Engineering -- Software product Quality Requirements and Evaluation (SQuaRE) --Evaluation process. International Organization for Standardization / ISO/IEC JTC 1/SC 7 Software and systems engineering, 2011.