Analysis of the Next Evolution of Security Audit Criteria

R Nykänen[1], T Kelo[2], T Kärkkäinen[1]

[1]*Faculty of Information Technology*
University of Jyväskylä
Jyväskylä, Finland

E-mail: riku.t.nykanen@student.jyu.fi; tommi.p.karkkainen@jyu.fi

[2]*Department of Pervasive Computing*
Tampere University of Technology
Tampere, Finland

E-mail: tomi.kelo@tuni.fi

Abstract: *Security assessments are performed for multiple reasons, including compliance with the information security regulation. Amongst other objectives, regulatory requirements are created to increase the resilience of national infrastructure and protect against information and cybersecurity threats. When the regulatory requirements are revised, the security audit criteria also need to be updated and validated. This was also the case with the Julkri, criteria developed for the conformance assessments of the renewed Finnish information security regulation. In this article, a comparative evaluation based on Design Science Research is performed to determine whether the new Julkri criteria improve existing criteria and control catalogues.*

Keywords: *Security Audit Criteria, Security Assessment, Information Security Controls, Design Science Research*

Introduction

Security controls are countermeasures that an organization implements to mitigate specific security risks. Security controls can be administrative, such as policies, processes, and training, or technical, such as endpoint protection software and backups. Organizations should implement cost-effective controls based on the risk assessment to mitigate their information and cybersecurity risks. The implemented controls are typically selected from a security control catalogue, which can be described as collections of the best practices for mitigating common information and cybersecurity risks.

Information security audits are used to assess the adequacy of organizations' information security from the compliance point of view. In the audits, a security control catalogue, such as ISO/IEC 27002 (International Organization for Standardization 2022b), NIST SP 800-53 (National Institute of Standards and Technology 2020), CIS Controls (Center for Internet Security 2021), or Katakri (National Security Authority of Finland 2020), defines the criteria that an organization is expected to meet. Security control catalogues are also regularly used when organizations assess their service providers or subcontractors to ensure the security of their supply chain.

The selection of used audit criteria and the security control catalogue are usually defined based on the security assessment. As an example, ISO/IEC 27002 is a widely adopted international standard by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) used as a part of ISO/IEC 27001 certification audits. As another example, NIST SP 800-53 is a U.S. national standard by the National Institute of Standards and Technology (NIST). The CIS Controls by the community-driven non-profit organization Center for Internet Security (CIS) is an example of a widely adopted reference control set without a status as a national or international standard. The Finnish Information Security Audit Tool Katakri is also a noteworthy example, being created in close cooperation between Finnish governmental security authorities and the private sector, with a focus on the protection of national classified information.

As organizations are different, management of information and cybersecurity is often risk-based, aiming to find the optimal controls for the current organization, the currently protectable assets, and/or a more strictly specified use case (Calvo & Beltrán 2022). Security risk management methodologies usually contain similar common phases (Fenz & Ekelhart 2011), where one essential phase is to analyse and select controls to mitigate the identified risks. For example, ISO/IEC 27001 requires an organization to "determine all controls that are necessary to implement the information security risk treatment option(s) chosen" and compare selected controls to ISO/IEC 27002, so that no necessary controls have been omitted. The risk-based approach allows the use of a control catalogue as a support mechanism to identify potential security controls. Performing effective risk identification, assessment, and mitigation for all assets seems to be extremely challenging even for organizations with adequate resources (McKeown 2019).

Where the private sector may have more freedom in the selection of suitable audit criteria for the specific purpose, the public sector is often more constrained to comply with the regulatory requirements. In this article, the authors analyse the process and outcomes of Julkri criteria (Information Management Board 2022) development using Design Science Research (Peffers *et al*. 2007). Julkri criteria were developed to provide a new tool for the conformance assessments of the renewed Finnish information security regulation, the Act on Information Management in Public Administration (906/2019) (Parliament of Finland 2019a), and the Government Decree on Security Classification of Documents in Central Government (1101/2019) (Parliament of Finland 2019b).

Security Audit Criteria and Control Catalogues

Security assessment

Compliance can be defined as the process of meeting expectations. More specifically, compliance is "verifiable consistency with clearly defined rules" (DeLong 2014). An information security assessment is the evaluation process to verify compliance against a set of rules. The set of rules is defined by the evaluation criteria used in the assessment. Information security audits can have multiple types of targets from organizations to specific products. Where the ISO/IEC 27001 (International Organization for Standardization 2022a) standard is a requirement specification for an Information Security Management System (ISMS), other specifications originate, for example, from regulatory or technical backgrounds. Hence, it is important to select a control catalogue adequate for the assessment.

The development, or update cycles, of security control catalogues occur typically in intervals of a few years. For example, the three versions of ISO/IEC 27001 were published in 2005, 2013, and 2022, and the last three versions of NIST SP 800-53 were published in 2009, 2014,

and 2019. Although the cybersecurity landscape evolves rapidly, the current update intervals of security control catalogues support the assessment purpose by improving stability in the requirements. Faster criteria update cycles could lead to an extra burden if the recertification interval is too stringent. Hence, updates to security control catalogues usually have accumulated needs for changes over several years.

When developing a new security control catalogue, there is no need to reinvent the wheel as several catalogues already exist. However, a rationale for a new catalogue is required. In the case of Julkri, the rationale was based on the need for compliance assessments against the updated regulations. With such a rationale, the content of the criteria must meet the regulatory requirements, although the basis for criteria can be formed from already existing specifications.

The semantics of security control catalogues

Security control structures vary in different frameworks. **Table 1** summarizes the previously presented control catalogue structures: NIST SP 800-53 release 5, ISO/IEC 27002:2022, CIS Controls v8, and Katakri 2020. The rationale for framework selection, instead of, for example, MITRE D3FEND, NIST Cybersecurity Framework, and BSI IT Grundschutz, is based on recent structural advancements of the selected frameworks.

	NIST SP 800-53 rel 5	**ISO/IEC 27002:2022**	**CIS Controls v8**	**Katakri 2020**
Control basic information	Identifier Name Control (text)	Identifier Name Control (text)	Controls: Number Title Safeguards: Number Title	Identifier Title Requirement(s)
Description	Discussion	Purpose Guidance Other information	Controls: Overview Why is this control critical? Safeguards: Description	Examples of implementation (as part of additional information)
References	External references Related controls			Legal references Other sources of information (as part of additional information)
Sub elements	Control enhancements		Safeguards	
Other attributes	Status (active or withdrawn)	Control type Information security properties Cybersecurity concepts	Controls: Procedures and tools Safeguards: Asset type	

		Operational capabilities Security domains	Security function Implementation group	

Table 1: Structural elements of security control catalogues

All selected catalogues have the following common basic elements for security controls: a unique identifier, control title, and description. ISO/IEC 27002:2022 has added five new attributes to controls compared to the previous version: control type, information security properties, cybersecurity concept, operational capabilities, and security domains. Attributes are intended to be used to create different views of a control catalogue to select appropriate subsets of controls.

A control type attribute describes how and when a control impacts the risk outcome and has the following possible values: *preventive*, *detective*, and *corrective*. The control type attribute is information that overlaps somewhat with the cybersecurity concept attribute, which can have the values identify, protect, detect, respond, and recover defined in the ISO/IEC TS 27101 "Cybersecurity framework development guidelines" standard draft and already implemented in the NIST Cybersecurity Framework. The information security properties define which information security properties, that is, confidentiality, integrity, and availability (CIA), are protected by the corresponding control (Yee & Zolkipli 2021).

The security domain is an attribute to view controls from the perspective of information security fields, expertise, services, and products. Attribute values consist of the following: *Governance and Ecosystem*, *Protection*, *Defence* and *Resilience*. The attribute is based on the needs of the European Union Directive 2016/1148 (also known as the NIS directive). The directive defines cybersecurity requirements for specific critical domains. The European Union Agency for Cybersecurity (ENISA) has produced equivalent mapping to ISO/IEC 27001 requirements and Annex A with the same attribute values. The operational capabilities describe aspects of the security operations, which are valid for the specific security controls. There are 14 possible values, including *Governance*, *Asset Management*, *Information Protection*, *Human Resource Security*, and *Physical Security*. The objective of the attribute is to be able to filter controls from the practitioner's perspective.

ISO/IEC 27002:2022 and CIS Controls include an additional shared attribute. CIS Controls include a *security function* attribute for each safeguard to define how the safeguard supports cybersecurity. Possible values, originally defined in the NIST Cybersecurity Framework (Barrett 2018), are as follows: *identify*, *detect*, *protect*, *recover*, and *respond*, where one of the values is set for each safeguard. ISO/IEC 27002:2022 has an attribute called *cybersecurity concept* that has the same values, but each control can have multiple values selected. CIS Controls also define attribute named asset type that describes the types of assets the corresponding safeguard protects. Asset taxonomy includes the following types: *Applications*, *Data*, *Devices*, *Network*, and *Users*, but some of the safeguards do not apply to every asset type (marked as N/A). Although the asset taxonomy is simple, it can be used similarly to the way ISO/IEC 27002:2022 uses operational capabilities.

The CIS Controls' structure differs from the other analysed frameworks in a significant way. Security control in CIS Controls can be seen as a high-level objective to ensure security in a specific function. Security control is, however, extended with definitions of multiple safeguards for each control. Safeguards can be characterized as more concrete activities to

ensure the objective defined by the security control. Safeguards are at a similar level as security controls in the other analysed frameworks. A similar high-level control objective was used in the previous versions of ISO/IEC 27002 but was removed from the 2022 version.

Like CIS controls, NIST SP 800-53 and Katakri have similar two-level approaches. NIST SP 800-53 controls have control enhancements, which can be seen as sub-controls, as they are structurally nearly the same as controls. Control enhancements always belong to specific security controls. Katakri has implemented levels within requirements in textual format and does not have similar structural elements. A single criterion (control) in Katakri can have multiple security requirements, but some of the requirements apply only to a certain security classification level. All three frameworks have implemented prioritization of security controls utilizing the presented structures. Where all controls are not applicable on all security or risk levels, the two-level approach enables primary control to be always active and applying the sub-elements only on suitable security levels.

Methods

The development of new Julkri criteria contained elements that resemble the Design Science Research (DSR) process. Although Julkri development did not claim to use DSR as a development framework during the project, the authors will evaluate the developed artefact based on DSR evaluation criteria. DSR is a research method that is used to develop a set of artifacts to solve a wicked problem. The iterative DSR process is composed of relevance, rigor, and design cycles (Hevner 2007) as presented in **Figure 1**.

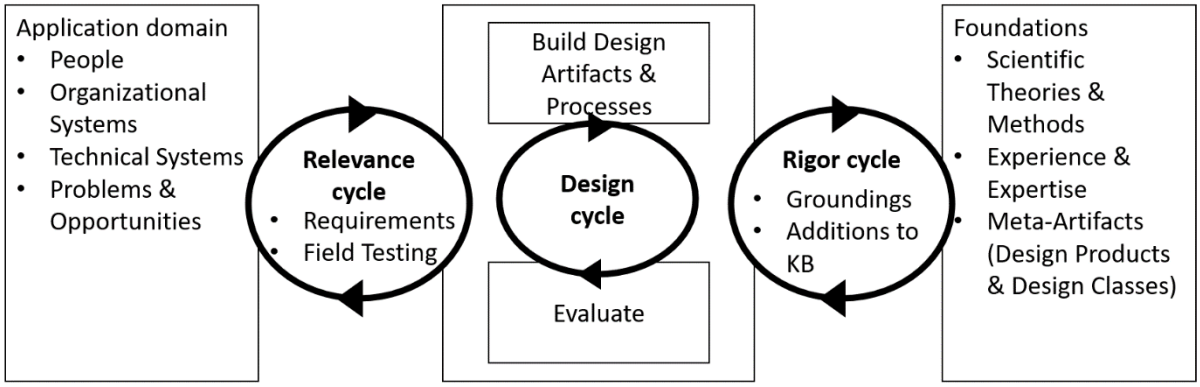

Figure 1: Design Science Research cycles (Hevner 2007)

The relevance cycle ensures that technology-based solutions solve important and relevant business problems, setting the requirements and acceptance criteria for research results. The rigor cycle provides the prior scientific knowledge and theories as a foundation for the research but also ensures that rigorous methods are applied in the construction and evaluation of the artifact. The design cycle research activities iterate between the construction of an artifact, its evaluation, and feedback to refine the design further (Hevner 2007).

In the Julkri development, the rigor cycle included the evaluation of recent development of related standards and methods. At the time of Julkri work, ISO/IEC 27002 version 2022 reached the approval stage where the Final Draft International Standard (FDIS) version was available for analysis. In addition to ISO/IEC 27002, also recently published NIST SP 800-53 release 5 was analysed in a rigor cycle for structural elements that could be used in Julkri. Where the rigor cycle concentrated on the structure, the relevance cycle focused more on the content of the Julkri criteria. Julkri's requirements are based on the legislation. Thus, the content

of the criteria is not expected to be equal to international standards or best practices as they contain security controls not arguable by legislative requirements. Still, the criteria must consider security controls usually expected to be implemented to ensure the information security requirements of the legislation.

As Julkri development contains typical elements of a DSR project to solve a wicked problem of legal conformance, the developed criteria shall be evaluated as a DSR artefact. DSR as a research method can have multiple goals, which require different evaluation strategies. Framework for Evaluation in Design Science (FEDS) addresses the lack of guidance to evaluate DSR research (Venable, Pries-Heje & Baskerville 2016). The authors utilize FEDS to create evaluation strategies to perform a comparative evaluation to determine if Julkri, as a DSR artifact, is an improvement, compared to other existing criteria and control catalogues. As evaluation is performed *ex-post* concerning the Julkri development; the summative evaluation strategy is used. Evaluation episodes are based on the DSR research goals (Venable 2010), which are complemented by security audit criteria evaluation principles (Kelo, Eronen & Rousku 2018). The authors utilize the Quick and Simple evaluation strategy, suitable for summative *ex-post* evaluation (Venable, Pries-Heje & Baskerville 2016). The Model for Efficient Development of Security-Audit Criteria (Kelo, Eronen & Rousku 2018) includes three phases of criteria development: design, implementation, and utilization. As the authors evaluate only Julkri as an artefact, the utilization phase from evaluation is excluded and the authors focus instead on the design and implementation phase.

Development of Julkri Criteria

Regulatory background

As multiple security control catalogues already exist, including national Katakri and PiTuKri (Finnish Transport and Communications Agency Traficom 2020), the need for Julkri was not evident. The rationale for Julkri development was based on the authoritative role and tasking of the National Information Management Board (IMB) (Information Management Board 2023).

As the IMB has the responsibility to define procedures based on the Act on Information Management in Public Administration, Julkri criteria were developed for compliance assessments. Regulatory requirements are generally written on a high abstraction level, which is not optimal for compliance assessments. To support the assessments, the criterion needs to refine the requirements on a more detailed level. These refinements were based on controls defined in standards and other best practices.

Julkri criteria content was initially based on Katakri and additionally on cloud security assessment criteria PiTuKri. The regulatory background of the latest Katakri version is the same as in Julkri (906/2019 and 1101/2019), focusing on the protection of classified information on levels RESTRICTED, CONFIDENTIAL and SECRET. Katakri also covers the protection of European Union Classified Information (EUCI). Scope for Julkri excluded protection of EUCI but included national TOP SECRET.

Development process

In the initial development cycles, activities of relevance and rigor cycles were executed in parallel. The initial version of criteria content was developed by the groups of subject experts as part of relevance and design cycles. The structure of the criteria was developed in the rigor cycle by the core development team. As the development work proceeded, more focus was on relevance and design cycles and less was on rigor cycles.

The initial content of Julkri was based on the Katakri with cloud security supplements from PiTuKri. Compared to the Katakri sections, new sections of “Preparedness and continuity management” and “Personal data protection” were introduced. After completion of the initial content, legislative validation was performed. At this phase, the phrasing of multiple criteria and recommendation texts was modified to meet the regulatory requirements more precisely.

The draft recommendation was open for comments via the public commenting service after legislative validation. Both public and private organizations were invited to provide their statements for the Julkri draft. In total, 32 organizations provided their responses to the proposal. Of these, 23 were public sector organizations, including, for example, municipalities, ministries, and government agencies. Seven of the responses were from private sector companies, including, for instance, global cloud service providers.

In general, the feedback was positive. Multiple responses indicated that criteria clarify the assessment of regulatory requirements. Also, the structure of the criteria and language used were found to be clear. In negative feedback, two issues were emphasized. First, the relationship and priority between the three different national criteria (Julkri, Katakri, and PiTuKri) was not seen to be clear. Secondly, the support for zero trust architecture was not seen as sufficient. Based on the feedback, the criteria were slightly modified. The structure and metamodel of Julkri did not receive negative feedback and were thus not modified.

Structure of Julkri

The final structure of the Julkri criteria can be divided into two main elements: the Julkri guideline document and the Julkri tool. The Julkri guideline document is composed of the following elements:

- Recommendation document - Background and guidelines on how to use Julkri
- Annex 1A - List of criteria as the text document
- Annex 1B - List of personal data protection criteria as the text document
- Annex 2 - Julkri tool (spreadsheet, not included in the document)
- Annex 3 - Julkri tools guideline
- Annex 4 - Glossary

Annex 1 was separated into two parts, 1A and 1B, after another legislative validation. The rationale was based on competencies; only the Office of the Data Protection Ombudsman (ODPO) is authorized to provide guidance on personal data protection in Finland. Hence, the domains under IMB and ODPO competencies were separated. The second main element of Julkri is the Julkri tool, which is an Excel spreadsheet. It contains criteria defined in Annex 1A and 1B in format, where criteria can be filtered based on preconditions. Preconditions are based on the criteria metamodel.

Criteria metamodel

Open Security Controls Assessment Language (OSCAL) defines a generic metamodel of control catalogues, control baselines, system security plans, and assessment plans and results. NIST SP 800-53 revisions 4 and 5 have been published in OSCAL format. In Julkri development, Katakri was used as a basis for the metamodel and hence OSCAL was not followed but was used in the evaluation. The Julkri metamodel and its comparison to OSCAL concepts are presented next.

The complete Julkri tool consists of five sections as described earlier, which each contain a set of criteria. Each criterion can have an additional sub-criterion to provide more detailed requirements or implementation guidance. This structure was adopted from NIST SP 800-53, which has a similar two-level control and control enhancement structure. In the initial version, it was allowed to have a recursive hierarchy of sub-criterion. It was however identified at a very early phase that a two-level structure was sufficient and easier to understand. Criterion and sub-criterion are structurally identical with the exception that the sub-criterion has additional reference to the parent criterion. It should be noted that all attributes are not mandatory, and many sub-criterions provide, for example, only additional implementation guidance for higher security levels. The attributes of a criterion are presented in **Table 2**.

Element	**Description**
Identifier	A unique identifier consisting of the abbreviation of the name of the sub-area, a consecutive number of the main criterion and, in a subcriterion, also a consecutive number of the subcriterion.
Name	The subject of the criterion
Requirement	The objective that the organization must meet. The requirement is a short sentence or a short paragraph.
Overview	Additional information that provides background and justification for the criterion.
Implementation guidance	Description of how the organization can implement the requirement. An implementation example is not a requirement, but it can serve as a guideline for the level of compliance with the requirement.
Confidentiality	Minimum confidentiality level when the criterion is expected to be applied.
Integrity	Minimum integrity level when the criterion is expected to be applied.
Availability	Minimum availability level when the criterion is expected to be applied.
Privacy	Minimum privacy level when the criterion is expected to be applied.
Legislation	The legislation on which the criterion is based.
References	References to the recommendations by the IMB, the PiTuKri assessment criteria and standards, including ISO/IEC 27002.
Julkri reference	A reference to one or more other relevant Julkri criterion.
Katakri reference	A reference to the corresponding criterion in the Katakri, if one exists.

Table 2: The attributes of a Julkri criterion

From these elements, confidentiality, integrity, availability, and privacy are later referred to as CIAP properties. During the rigor cycle, an analysis of existing classifications, especially for integrity and availability, were conducted, and the scale was implemented based on the findings. For confidentiality and privacy, scales were already defined in the legislation. **Figure 2** presents the Julkri metamodel as a UML diagram.

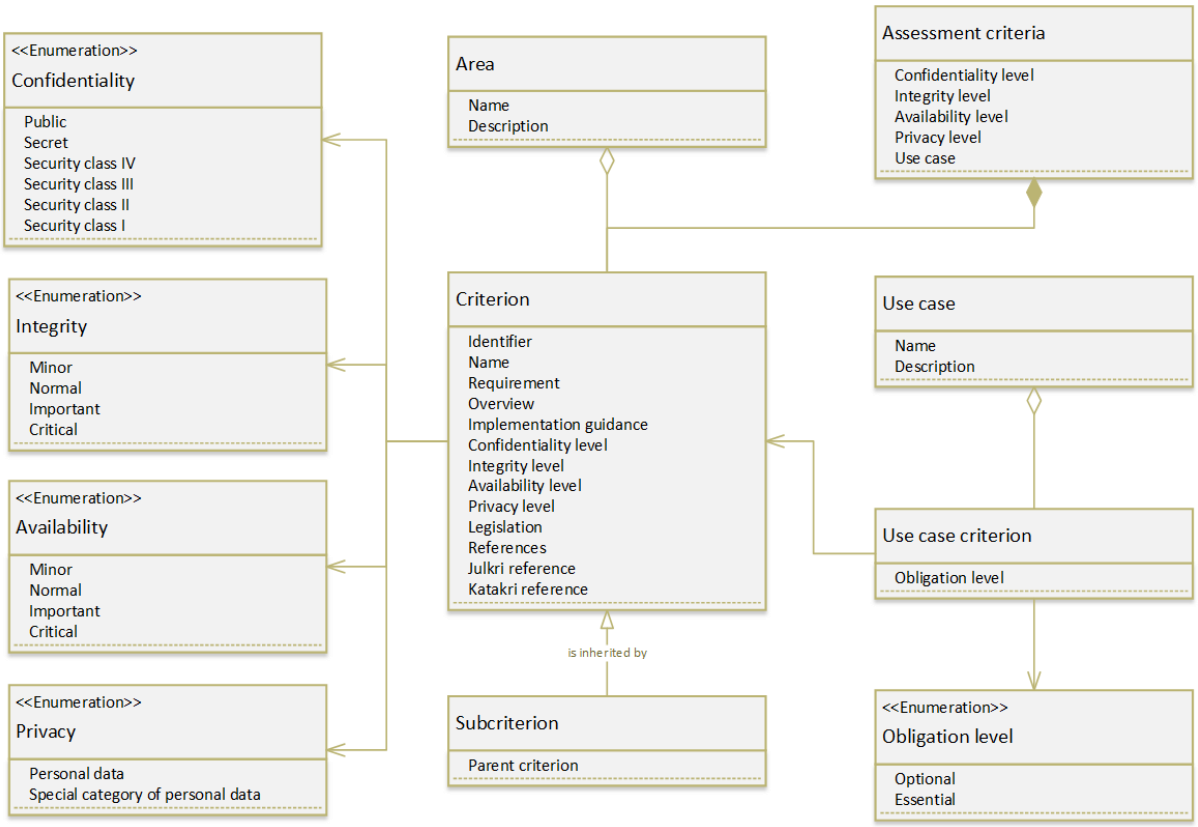

Figure 2: Julkri metamodel

OSCAL concepts were analysed in the rigor cycle as one input for the meta-model design. The concept of profiles had an especially significant impact on the use case concept of Julkri. **Table 3** presents a mapping of Julkri concepts to OSCAL concepts.

OSCAL concept	**Julkri concept**
Catalog	Criteria
Profile	Use case
Group (Family)	Area
Control	Criterion
Control enhancement	Sub-criterion

Table 4: Mapping of OSCAL and Julkri concepts

The global or control parameters concepts of OSCAL, as utilized in NIST SP 800-53 rev 5, were not included in Julkri. The rationale is two-fold: Julkri is not expected to be utilized by other specifications, but to be adapted via use cases. On the other hand, the functionality of control parameters is implemented using sub-criterion refining the main criterion.

Adapting a risk-driven approach

Applying regulatory requirements for a risk-driven approach was analysed during the rigor cycle. As a result, OSCAL control layer concepts were used to implement the risk-driven approach. Compared to Katakri and PiTuKri, utilizing only the confidentiality of information as selection criteria, Julkri's approach was more versatile.

First, Julkri's concept of use case is like the OSCAL profile and NIST Risk Management Framework concept of overlays. Julkri use cases are used to define a subset of criteria that is relevant to a specific purpose. The OSCAL profile is a binary approach to include or exclude a control from a profile. However, in Julkri, the use cases have three options: essential, optional, or excluded. Essential criteria are considered mandatory to be complied with, but they can be compensated with other controls. Each optional criterion shall be evaluated based on risk—to be included in the assessment or not. Excluded criteria are scoped out.

In addition to the predefined use cases, customised use cases can also be defined. The first version of Julkri criteria contains four common use cases:

- Public Administration Unit security assessment
- SaaS cloud service security assessment
- Professional services security assessment
- IT service provider security assessment

The risk-driven approach is implemented in Julkri using use cases and CIAP properties, which are used as input for criteria selection. Selection logic is shown in **Figure 3**.

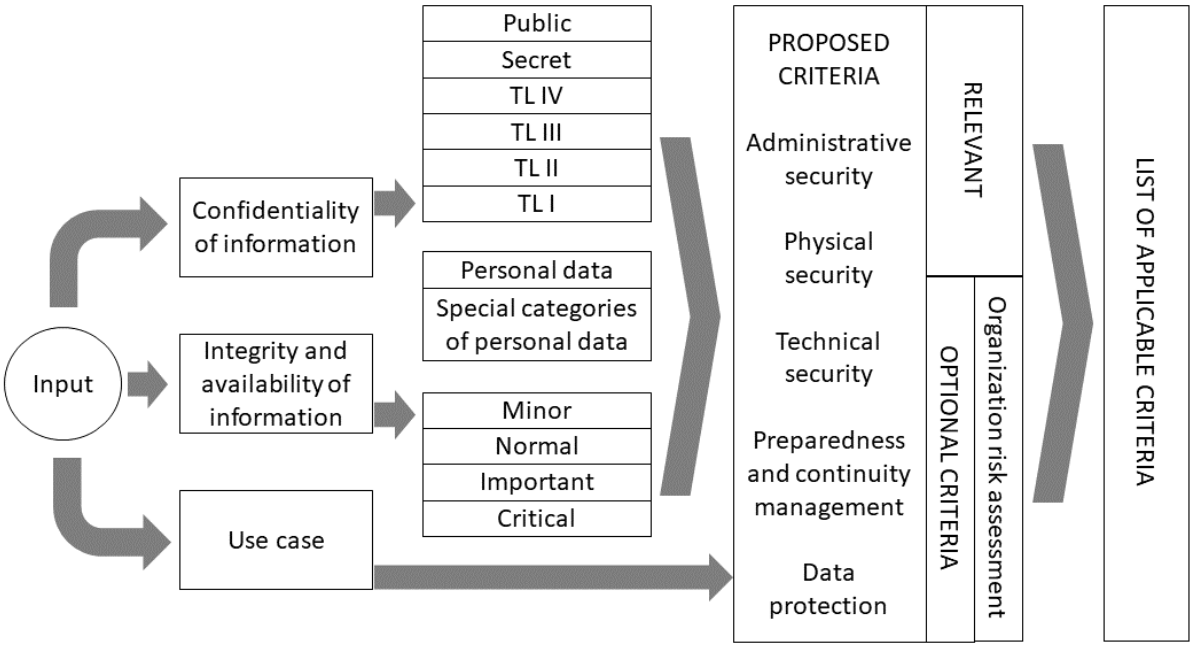

Figure 3: Illustration of selecting the applied criteria (Information Management Board 2022)

The number of essential criteria is fairly small compared to the number of optional criteria as it requires both the use case and CIAP property to be essential for the criterion. Criterion will be optional if CIAP property or use case is optional. Criterion is excluded only if none of the properties is essential or optional. This approach emphasizes the necessity of risk assessment to select the optimal set of security controls to be implemented.

Validation of criteria

During the finalization of the criteria, the coverage of contents was analysed against ISO/IEC 27001, ISO/IEC 27002, and PiTuKri. The purpose of the validation was to ensure that Julkri is not lacking essential requirements. Analysis can be considered as "triad verification", as regulatory requirements were also considered while evaluating correspondence. For example,

ISO/IEC 27002:2022 contains several security controls that are not covered by Julkri due to a lack of regulatory requirements. Additional verification was also performed against Katakri to ensure that no essential original Katakri content had been deleted or modified during the development process.

Evaluation of Julkri artefact

Next, the authors evaluated Julkri against design (IDs 1-3) and implementation (IDs 4-10) phase guidelines (Kelo *et al.* 2018). Utilization phase guidelines (IDs 11-16) are partially outside of the scope of the development project but are included in the analysis when applicable.

ID 1: Criteria design should stem from a small set of carefully selected and strictly defined use cases.

The guideline defines that criteria should limit the number of supported use cases and target groups to avoid balancing between requirements of different use cases and interests leading to a useless assessment tool. It is evident that the approach of Julkri is different from the evaluation guideline. By introducing a use case as a structural element and utilizing control selection using CIAP properties, Julkri can be adapted to multiple use cases and supports user organizations to adopt it to their specific use cases. As Julkri's use case is based on the OSCAL concept of overlays, it can be argued that is this a false negative finding as a similar approach is used also in the other criteria (Venable, Pries-Heje & Baskerville 2016).

ID 2: Use cases should be defined early in the criteria-development process. The validity of use cases should be ensured throughout the process.

Like guideline ID 1, Julkri's approach is different. Where its successors Katakri and PiTuKri have strictly defined use cases, Julkri contains more requirements from which a subset can be selected for a specific use case.

ID 3: Criteria should have an understandable scope and a reasonable number of requirements.

The scope of Julkri is to assess the fulfilment of the information security requirements laid down in the Information Management Act, Security Classification Decree, and partly also in the General Data Protection Regulation. Feedback from the public commentary period indicated that the relationship and status compared to other existing criteria was not clear, also indicating possible shortcomings in scope definitions and guidance on the proper use of the criteria.

ID 4: Common risks related to the use cases should be identified. The required controls should cover these risks.

The initial content of Julkri was based on the established Katakri and PiTuKri frameworks, and the content was also verified against ISO/IEC 27001 and ISO/IEC 27002:2022 standards. As some of the supported use cases are similar, also many of the use case specific risks are expected to be similar, and thus sufficiently covered. This does not however guarantee that all risks related to all use cases would be covered.

ID 5: Security criteria should describe minimum requirements but should also provide support for the security and risk-management processes of the target groups.

Julkri makes a noteworthy enhancement to the risk-driven approach by introducing a logic to select the minimum and optional risk-based requirements. The approach requires competence in risk management to select valid optional requirements. Without sufficient competence, the

approach may lead to unwanted situations. As an example, an organization may only comply with mandatory minimum requirements, and fail to identify a need for additional controls even in high-risk use cases. The development process did not include testing with various user organisations, emphasizing the need for further analysis after practical usage.

ID 6: Each criteria requirement should be justifiable for the use cases.
All requirements were formulated by groups of subject matter experts and were based on established frameworks. From the DSR perspective, the public comment period can also be seen as a verification method to avoid, for example, biased views by experts or other criteria. In the case of Julkri, the comments did not include feedback that any requirement would be obsolete or not justifiable for the use cases.

ID 7: Requirements should be described at a reasonably concrete abstraction level.
Julkri's content was based on existing established criteria and standards, including the selected level of abstraction. Feedback gathered from the public commentary indicated the need for only a few clarifications.

ID 8: Criteria should be internally consistent.

Julkri´s approach was to use requirements from established existing criteria and to split the requirements into more atomic requirements where appropriate. The approach enabled cross-referencing and comparison of the requirements on an atomic level. The approach made also internal inconsistencies clearly visible and effectively fixable.

ID 9: Authoritative sources should be referenced clearly.
As the meta-model shows, Julkri contains references to regulatory sources of requirements. Also, the authoritative role of the IMB was clearly stated in the criteria.

ID 10: The requirements should be compared to those of similar criteria to reveal possible biases.
Requirements were based on established similar criteria and were also verified against similar criteria and standards. Although no noteworthy biases were identified, the remark was made on non-similar use cases in criteria and standards selected for comparison, which may leave some biases unnoticed.

ID 11: Thorough practical testing of the criteria should be conducted before publication.
Julkri's development did not include an extensive practical testing phase. As Julkri was mainly based on an established, extensively tested Katakri framework, it was expected that no major findings would have been found in the practical testing of Julkri. On the other hand, Julkri also introduced support for use cases not supported in Katakri, and testing such use cases might have been justified.

ID 13: Instructions for proper usage within each of the use cases should be provided.
Julkri has extensive guidelines included as part of the main document release. In addition to guidance included in the recommendation document, the document has also Appendix 3, which includes instructions on how to use the Julkri Excel tool.

ID 14: Appropriate guidance and training should be offered to unify the interpretation of criteria.

At the time of publishing Julkri, there was no training material available. The development of training material, however, began after the publication.

ID 16: Criteria should be made available to the target groups.
Julkri is publicly available on IMB's website, free of charge.

Themes covered in guidelines ID 12 (Effort should be expended to gain recognition for the criteria) and ID 15 (Audits of critical targets should be limited to certified practitioners to ensure sufficiently reliable results) were outside of the scope of the Julkri development and were thus not evaluated in this research.

Results and discussion

Summary of the results:

- The use of established frameworks can operate as an efficient starting point for new criteria.
- The designed metamodel of Julkri supports several enhancements compared to many existing frameworks. As an example, a risk-driven approach can be supported by introducing a logic to select the minimum and risk-based additional controls. As another example, the amount and variety of supported use cases may be flexibly expanded by metamodel design and atomicity of criteria requirements.
- The public comment period is an essential method to verify the applicability of DSR artefacts to real-world scenarios.
- The Julkri development process did not include testing with various user organisations, emphasizing the need for further analysis after practical usage.

When considering criteria development guidelines ID 1 and ID 2, the security control catalogues and security audit criteria can be divided into two categories: general catalogues and use case specific catalogues. General catalogues can be adapted for use case specific needs using approaches like OSCAL profiles and control parameters while supporting many use cases. Further research is needed to analyse whether the use case specific approach provides a more understandable and practically efficient tool for various user groups, or whether similar results can be achieved with adapted general catalogues.

When evaluating guidelines ID 11, ID 13, and ID 14, it seems evident that the development of Julkri criteria should have included practical testing as well as the creation of training materials. If Julkri is being taken into practical use by the target groups, their experiences could provide valuable input for further research. Future research topics could focus especially on utilization phase guidelines (IDs 11-16), and could cover, for instance, efforts made to gain recognition of the criteria (ID 12). Analysis of ID 12 would be needed especially if the Julkri criteria is being taken into practical use parallel or in conjunction with the other established frameworks.

Future research would also be needed on the practical implementations of the risk-driven approach. The introduced logic to select the minimum and risk-based additional controls especially requires further validation. A validation is recommended in practical use cases, covering the soundness of the logic, understandability for the users, and the sufficiency of resulting protection against security risks currently faced by user organisations.

References

Barrett, M 2018, 'Framework for Improving Critical Infrastructure Cybersecurity', version 1.1, *NIST Cybersecurity Framework*, National Institute of Standards and Technology, Gaithersburg, MD, US.

Calvo, M & Beltrán, M 2022, 'A model for risk-based adaptive security controls', *Computers & Security*, vol 115.

Center for Internet Security 2021, *CIS Critical Security Controls*, 8th ed, viewed 20 February 2023, <https://www.cisecurity.org/controls>.

DeLong, J 2014, 'Aligning the compasses: A journey through compliance and technology', *IEEE Security & Privacy*, vol. 12, no. 4, pp. 85-9.

Fenz, S & Ekelhart, A 2011, 'Verification, validation, and evaluation in information security risk management', *IEEE Security & Privacy*, vol 9, no. 2, pp. 58-65.

Finnish Transport and Communications Agency Traficom 2020, *Criteria to Assess the Information Security of Cloud Services (PiTuKri)*, edition 1.1, ISBN 978-952-311-505-7, Traficom publications, Helsinki, Finland.

Hevner, AR 2007, 'A three-cycle view of design science research', *Scandinavian Journal of Information Systems*, vol. 19, no. 2, pp. 87-92.

Information Management Board 2022, *Assessment criteria for information security in public administration (Julkri): Recommendation and criteria*, 1st ed., Publications of the Ministry of Finance, Ministry of Finance, Helsinki, Finland.

—2023, Ministry of Finance, viewed 20 February 2023, <https://vm.fi/en/information-management-board>.

International Organization for Standardization 2022a, *Information security, cybersecurity and privacy protection, Information security management systems, Requirements*, ISO 27001:2022 edition, International Organization for Standardization, Geneva, Switzerland.

—2022b, *Information security, cybersecurity and privacy protection—Information security controls*, ISO 27002:2022 edition, International Organization for Standardization, Geneva, Switzerland.

Kelo, T, Eronen, J & Rousku, K 2018, 'Enhanced model for efficient development of security-audit Criteria, *Journal of Information Warfare*, vol. 17, no. 3, pp. 50-63.

McKeown, DA 2019, 'Building a risk-based information security culture', *ISSA Journal*, vol. 17, no. 4, pp. 14-21.

National Institute of Standards and Technology 2020, *Security and Privacy Controls for Information Systems and Organizations, Special Publication 800-53*, 5th ed., National

Institute of Standards and Technology, Gaithersburg, MD, US.

National Security Authority of Finland 2020, *Katakri 2020: Information Security Audit Tool for Authorities*, ISSN 2669-8757, Finnish Transport and Communications Agency Traficom, Helsinki, Finland.

Parliament of Finland 2019a, *Act on information management in public administration (906/2019)*, Ministry of Finance, Finland, viewed 20 February 2023, <https://www.finlex.fi/en/laki/kaannokset/2019/en20190906.pdf>.

—2019b, *Government Decree on Security Classification of Documents in Central Government (1101/2019)*, Ministry of Finance, Finland, viewed 20 February 2023, <https://www.finlex.fi/en/laki/kaannokset/2019/en20191101.pdf >.

Peffers, K, Tuunanen, T, Rothenberger, MA & Chatterjee, S 2007, 'A design science research methodology for information systems research', *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45-77.

Venable, J, Pries-Heje, J & Baskerville, R 2016, 'FEDS: A framework for evaluation in design science research', *European Journal of Information Systems*, vol. 25, no. 1, pp. 77-89.

Venable, J 2010, 'Design science research post Hevner *et al.*: Criteria, standards, guidelines, and expectations', *Global Perspectives on Design Science Research, DESRIST 2010, Lecture Notes in Computer Science*, eds. R Winter, JL Zhao & S Aier, Springer, Berlin, Heidelberg, Germany, pp. 109-23.

Yee, CK & Zolkipli, MF 2021, 'Review on confidentiality, integrity and availability in information security', *Journal of ICT in Education*, vol. 8, no. 2, pp. 34-42.