

# Translating NIS2 Requirements into Actionable Tasks for SMEs Using STRNIS2

Imants Breidaks<sup>1</sup>, Henrijs Kaļķis<sup>2</sup>,  
Anton Semenov<sup>3</sup> and Valdis Porneiks<sup>4</sup>

<sup>1</sup> University of Latvia, Faculty of Medicine and Life Sciences, Riga, Latvia

<sup>2</sup> University of Latvia, Faculty of Business, Management and Economics, Riga, Latvia

<sup>3</sup> Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine

<sup>4</sup> LLC Stratex, Latvia

Correspondence: [imants.breidaks@lu.lv](mailto:imants.breidaks@lu.lv)

## ABSTRACT

Organisations must translate cybersecurity requirements into work that people can carry out and managers can check. This methods paper specifies STRNIS2, a six-stage method for assigning that work in small and medium-sized enterprises. Its Human-Centric Compliance Matrix (HCCM) records the requirement, task, responsibilities and evidence. The method develops our earlier NIS2 Compliance Starter Pack by specifying how information and effort are allocated across a handover. A purposive document analysis connects European and Latvian requirements with human-factors research and incident-response guidance. In a constructed reporting example, information may be deferred only if it is unnecessary for an immediate safe decision, a capable recipient accepts the remaining work, and recording and notification deadlines remain achievable. Comparison with an existing shared ticket examines when to change a procedure and when to retain it. A planned five-case study will assess method use through paired task-structuring sessions, Raw NASA-TLX, interviews and documentary review. The contribution is a task-design method and review procedure; effects on workload and cybersecurity remain to be tested.

**Keywords:** NIS2, human factors, SMEs, work-system design, compliance tasks, NASA-TLX

## INTRODUCTION

An employee notices that shared production files have become unreadable. The company has an incident procedure, but the employee must choose between several reporting routes and complete a form asking for information they do not have. What must this person do now, and what work belongs to the person receiving the report? This hypothetical situation exposes a design decision that a policy title cannot resolve.

NIS2 requires proportionate cybersecurity risk management, incident handling, effectiveness assessment and management oversight. Latvia implements these duties through the National Cybersecurity Law and Cabinet Regulation No. 397. Section 25 of the law makes the organisation's head responsible for cybersecurity management and requires a designated cybersecurity manager. The regulation specifies minimum requirements, including incident procedures and records. Applicability depends on activity, size and relevant exceptions or designation (European Parliament and Council, 2022; Saeima, 2024; Cabinet of Ministers,

Received August 30, 2026 Revised September 10, 2026 Accepted September 14, 2026 Available online September 25, 2026

2025). This paper concerns SMEs whose applicable duties have been established and whose specialist capacity is limited.

Our earlier AHFE paper introduced a four-phase NIS2 Compliance Starter Pack connecting human factors, control design and evidence (Breidaks et al., 2026). This paper specifies the method for examining one task within that process. STRNIS2 means Socio-Technical Resilience for NIS2; HCCM means Human-Centric Compliance Matrix. We ask how an SME can assign a regulated task across roles and record the reasons for that assignment. The contribution is a method specification and analysis of a constructed example. The case study is planned as part of the first author's doctoral research.

## RELATED WORK AND DESIGN BASIS

Existing methods provide several starting points. Productive Security uses interview-informed, scenario-based surveys to examine employee behaviour and policy implementation (Beautement et al., 2016). MORPHEUS connects human factors with measurement instruments and operational scenarios for diagnosis and intervention (Desolda et al., 2026). STS-CROP addresses sociotechnical IT/OT risk management (Imran et al., 2026), while CyberESP develops an SME framework through an asset-management artefact (Calvo-Manzano et al., 2025). These approaches already address practical decisions. STRNIS2 focuses on the assignment of one task: what each role must know and do, whether it can do so, and which evidence supports that arrangement.

For the reporting example, the closest comparisons concern incident information and response arrangements. Michalek et al. (2026) review SME incident prevention and response. The AIR preprint specifies information to capture during OT incidents (Vidal et al., 2025), and NIST SP 800-61 Rev. 3 describes response roles and information sharing (Nelson et al., 2025). STRNIS2 uses this guidance to examine a handover between people with different knowledge and capacity. HCCM records the allocation decision, its source and the conditions that would make it unsafe or impractical. Its added value depends on whether that examination identifies a consequential problem that the existing procedure leaves unresolved.

SEIPS 2.0 examines the interaction between people, tasks, tools and organisational conditions (Holden et al., 2013). We use this perspective to ask whether the assigned work fits the available roles, resources and time; we do not transfer healthcare findings to cybersecurity. Hielscher et al. (2023) show that security managers may recognise problems without having the support to resolve them. Naming an owner therefore leaves a further question: does that person have the authority and capacity to act?

Response cost refers to the effort, time or inconvenience associated with protective action (Kiran et al., 2025). Here it guides questions about what a control requires from the person using it. We do not test the full protection-motivation theory. NASA-TLX instead measures the workload experienced during a task (Hart, 2006). Task demands also differ from accumulated security-related strain (Mullins and Thompson, 2026), so a lower workload rating would not by itself establish reduced security fatigue.

We assembled a purposive source set from the existing research bibliography, a search for relevant comparator methods and official legal texts. Sources were selected to establish a duty, explain a work-system problem, inform incident response or compare a design approach. Title and DOI searches through publisher and author-repository records checked publication identities. For four central choices in the example, Table 2 records the source provision, our design inference, an alternative or failure condition, and the reason to reject or revise the choice. This makes the reasoning open to examination. The legal basis is the text applicable on 5 September 2026. The study provides a formative analysis of a constructed design (Venable et al., 2016).

## THE STRNIS2 METHOD

STRNIS2 examines one task with a trigger, performer, sequence and identifiable result. The cybersecurity manager works with the process owner and people who perform it. The task is selected after the organisation's applicable duties have been assessed; selecting it does not narrow those duties. Work passed to another person remains part of the analysis. The six stages are as follows.

**1. Establish the requirement.** Record the applicable provision, version, scope decision and required outcome. Separate the organisation's obligation from the action expected of a particular employee.

**2. Describe the work.** Identify the trigger, steps, tools, roles and handovers from process documents and accounts of practice. Record competing work and relevant dependencies. Include safety, continuity or supplier constraints where they affect this task.

**3. Identify the difficulty.** State a specific proposition and its basis. A problem observed in local records, a finding transferred from research and an author's hypothesis have different evidential status. Consider alternatives such as missing authority or unavailable support before attributing delay to workload.

**4. Adapt the control.** Compare the existing process with a candidate change. Preserve the required outcome, consider what a well-specified existing procedure already achieves, and identify whose work increases or decreases. Retaining the existing process is a legitimate decision.

**5. Assign responsibility and evidence.** Identify who performs, receives and authorises the work, and who maintains its record. Separate implementation evidence from an effectiveness check. Specify the check's conditions and acceptance criteria before it is run.

**6. Check and revise.** Examine tests, incidents, deviations or unresolved assumptions against those criteria. Record what failed, the corrective owner and the next review. A proposed check remains marked as unperformed until evidence exists.

The earlier four phases describe the overall compliance process. These six stages specify how to examine one task within it, separating legal scope from work description and assigning responsibility for evidence and review. HCCM is the working record used throughout the stages.

## The record produced by the method

Table 1 defines what HCCM records. Each group needs an entry or a reference to an existing procedure. Add context only where it affects the task. Unresolved items need an owner and review date; they remain unresolved until the necessary evidence is available.

**Table 1.** HCCM field definitions for one task.

| Field group              | Content to record                                                                                                    |
|--------------------------|----------------------------------------------------------------------------------------------------------------------|
| Requirement and scope    | Provision and version; applicability basis; required outcome.                                                        |
| Task and work setting    | Trigger, performer, steps, tools, result and next handover; relevant constraints and dependencies.                   |
| Difficulty and basis     | Possible failure; source or local evidence locator; observed, transferred or proposed status; competing explanation. |
| Control and alternative  | Current and candidate designs; reason to change or retain; information and effort reassigned; safeguards preserved.  |
| Responsibility           | Performer, recipient and decision owner; authority, capacity and fallback responsibility. Roles may be combined.     |
| Implementation record    | Implementation status; record or procedure reference, storage location and maintainer.                               |
| Effectiveness check      | Test condition, acceptance criterion, result locator or “not yet tested”; who conducts the check.                    |
| Review and residual risk | Unresolved dependency or risk; corrective owner, review date or trigger; record-update responsibility.               |

## WORKED EXAMPLE: INTERNAL INCIDENT REPORTING

The constructed setting is a medium-sized Latvian manufacturer of electrical equipment, assumed to be confirmed in scope. A production planner finds shared schedules and quality records encrypted. The planner can describe the symptom and interrupted work, but does not know the cause or full impact. The process under examination requires a complete form before escalation. This is an assumed difficulty, not a finding about manufacturers.

The task starts when the planner recognises the abnormal event. It ends when the designated recipient confirms the handover and can act. An automatic receipt confirms submission but leaves the recipient’s availability uncertain. If handover is not confirmed within the time set by the incident procedure, the reporter uses the designated fallback. Assessment, completion of records and any external notification follow as assigned tasks. Where immediate safety action is required, staff follow the company’s established procedure without waiting for paperwork.

Regulation No. 397, paragraph 46, addresses incident processes, responsibilities and communications. Paragraph 47 requires incident-log entries within 24 hours of detection or changes to recorded information. Paragraph 48 specifies log content, with actual incident time and causes or indicators qualified by “if known” (Cabinet of Ministers, 2025). These are not instructions that the first reporter must establish the cause. Nor does the logging deadline justify delaying internal escalation; it is distinct from the external notification process.

### A proposed rule for allocating information

Our proposed rule is to assign information to the person who can supply it at the stage when it is needed. An item may be deferred only if three conditions hold:

- (C1) Safety: the item is unnecessary for an immediate safe decision;
- (C2) Capacity: a capable recipient accepts the remaining work;
- (C3) Deadlines: recording and notification deadlines remain achievable.

The rule concerns how work is assigned; a shorter first report is one possible consequence.

Before use, the organisation must check which information its initial decisions actually require. For this example, the first report conveys what is known about the discovery time, affected system, visible symptom, interrupted work and contact person. If information needed for an immediate decision is unknown, the report flags that uncertainty for urgent assessment. It must not require a guess or delay escalation. The recipient obtains the missing information, assesses the event and maintains the incident record. A field cannot be deferred merely because it is inconvenient to answer. Table 2 records how each design decision follows from a source provision and which condition of the rule it implements; the last column states, in advance, the observation that would require rejecting or revising the decision.

**Table 2.** Source-to-design derivation. Design choices and rejection conditions are author propositions.

| Basis                                                             | Decision in the example                                                                                        | Implements | Condition requiring rejection or revision                                                 |
|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|------------|-------------------------------------------------------------------------------------------|
| Reg. 397, 46.1 and 46.3; NIST GV.RR-02                            | Assign a receiving role with authority and cover; use accepted handover as the task boundary.                  | C2         | A named recipient cannot act, or the fallback has the same unavailable dependency.        |
| Reg. 397, 48.1 and 48.4; stated limits of the planner's knowledge | Do not require an unknown cause or exact incident time before the initial report.                              | C1         | Deferral withholds information already known and necessary for a safe immediate decision. |
| Reg. 397, 47-48                                                   | Assign completion and updating of the incident record to the receiving process.                                | C3         | Later work remains unassigned, required content is omitted, or recording is late.         |
| NIST DE.AE-06; work-system perspective in Holden et al. (2013)    | Make event information accessible to authorised responders; check channel availability and receiving capacity. | C2         | The message is submitted but inaccessible, unmonitored or left with an overloaded role.   |

The rejection conditions illustrate how the proposed allocation can fail to satisfy the rule or its associated implementation requirements. NIST SP 800-61 Rev. 3 supports defined response authority and access to event information for authorised

personnel or tools (Nelson et al., 2025, GV.RR-02 and DE.AE-06). The first-report fields, acknowledgement rule and fallback proposed here are local design choices, rather than requirements prescribed by that guidance. The HCCM entry remains “proposed; not tested”.

### **Comparison and failure conditions**

In the full-form process, the planner must answer investigation questions before reporting. Staging the report removes that obstacle but leaves the investigation and recording work to be done. If the recipient lacks time, access or authority, the delay moves to that person. Where one person performs both roles, staging changes the order of work without adding capacity.

Consider instead an existing shared ticket that accepts unknown values, fills known system details automatically, assigns a monitored recipient and provides an accessible fallback. It could meet the same objective without another form. Under STRNIS2, the company should retain that arrangement unless the review identifies a relevant gap. A difference in layout alone is no reason to replace it.

Three variations expose the limits of both designs. If only the cause is unknown, the initial report can proceed and the recipient investigates it. If the planner knows that a production line depends on the affected records, and that fact is needed for a safe immediate decision, neither design may defer it. If the reporting platform is unavailable, a second address on that same platform provides no fallback. Either design then needs an available route and a recipient who can act. These are deductions from the stated scenario conditions, not observations of company performance. They show why unknown information, necessary information and unavailable support require different decisions.

A later operational exercise would compare time to accepted handover, missing or incorrect decision-relevant information, routing errors and record completion. It would test channel and recipient unavailability against criteria set from the company’s needs in advance. Faster initial reporting would be unacceptable if it left an unsafe decision, an unaccepted handover or incomplete required records.

### **PLANNED EMPIRICAL EVALUATION**

The next stage follows the doctoral design: five purposively selected Latvian SME cases, one focal task and questionnaire participant per case, and formative review by five experts in human factors, NIS2 requirements or SME practice. Cases retain contrasts between internal and outsourced roles and IT-only and IT/OT settings. Experts will review clarity, omissions and practical barriers before the method version is fixed. The study examines whether practitioners can produce defensible task specifications. Eligibility and session rules will be fixed after formative review and before the case sessions. Any later changes will be documented with their reasons.

### **Paired task-structuring sessions**

These paired sessions examine whether a practitioner can produce a task specification with STRNIS2 and what effort that structuring work requires, compared with the company’s usual approach. Workload is measured with NASA-TLX, a standard subjective workload questionnaire in which the respondent rates

a just-completed task on six dimensions (Hart, 2006); we use the unweighted Raw variant because it is quicker to administer and keeps the session burden low.

A focal participant will structure the task using the company's usual approach and then complete Raw NASA-TLX. After a standardised 15-minute introduction, the participant will structure the same task with STRNIS2/HCCM and complete Raw NASA-TLX again. Both phases use the same source material and objective; the baseline may use normal company tools. The researcher will not provide a solution or coach either phase. Duration, interruptions and help requests will be recorded. A phase ends when the participant considers the specification complete or cannot progress with the available information; the stopping reason and unfinished work are recorded.

Raw NASA-TLX retains mental, physical and temporal demand, perceived performance, effort and frustration, each rated 0-100. The unweighted mean accompanies the dimension scores; a higher performance rating indicates poorer perceived performance. The instructions and coding remain identical across phases. These ratings concern the task-structuring session just completed, not the operational reporting task.

The same six questionnaire statements, rated before and after method use on a five-point agreement scale, concern clarity of roles, steps and expected evidence, suitable tools, available time and reasonable effort. An open response, one or two interviews per case and process documents will help explain clarification, remaining uncertainty and additional work.

### **Completeness is not correctness**

A 0-3 structural count awards one point each for a responsible role, a sequence with a trigger and result, and an evidence object with its storage location. It records presence only. HCCM explicitly prompts these elements, so a higher count cannot establish methodological value. SME research comparing self-reports with expert and technical assessment reinforces the need to examine what a record actually supports (Chidukwani et al., 2026).

A substantive review will therefore assess both phase outputs against the same criteria, irrespective of format. Legal and technical correctness concerns whether the interpretation preserves the applicable duty and control objective. Practical feasibility concerns whether named roles have the authority, tools, capacity and fallback needed, including work transferred to others. Evidence traceability concerns whether the proposed record and check answer the stated question and can be produced, located and maintained.

The reviewer will first judge individual claims as “supported”, “contradicted” or “unresolved”, giving a source locator and reason. Missing evidence is unresolved. For each criterion, a contradicted claim determines the overall label; otherwise an unresolved claim does; “supported” requires support for every applicable claim. Individual findings remain visible. An essential dependency is a condition without which the required outcome, necessary safeguard or handover cannot be achieved. A critical contradiction or unresolved essential dependency blocks recommending operational use. The review record will state the dependency, reason, decision and corrective owner. These rules guide formative review; they are not a validated scale.

The researcher will review outputs before seeing participant ratings and retain contrary evidence, ambiguities and new errors. A missing document will not be treated as missing practice without corroboration. Because the researcher knows the phase, the assessment is neither blinded nor independent. A useful change must go beyond filling the form: for example, records or a relevant role holder might confirm that the baseline assigned work to someone without access. Such corrections will be considered alongside the effort required and any new problems introduced.

Analysis will compare outputs within each case and then examine recurring or context-dependent patterns. The usual approach comes first so that baseline work precedes exposure to HCCM; reversing the order would risk carryover. Workload differences will be reported descriptively: repeating the same task and learning the material compete with the method as explanations. Interviews can clarify these explanations but cannot remove the confounding. Five cases support formative refinement. These sessions measure the effort of using the method; operational task performance and long-term record maintenance require separate assessment.

Fieldwork will require the institutional ethics process, organisational permission and participant consent. Collected records will be minimised and de-identified, excluding credentials and unnecessary exploitable details. No live incident or operational reporting exercise is required by this protocol.

## DISCUSSION

The method requires a company to explain who will do the work, what they need and why the arrangement should work. HCCM keeps that explanation alongside its sources and proposed checks. The reporting example makes the consequence clear: removing a question from the first form assigns work elsewhere. The change is reasonable only if the next person can do that work in time and maintain the required records.

HCCM also takes time to complete and maintain. If an existing procedure already answers the relevant questions, another record may add effort without improving the task. The useful outcome is a justified decision to change or retain the process, rather than a larger set of documents.

This study provides document-based reasoning and a constructed comparison. The purposive selection has no complete reproducible search log, and some comparisons rely on published summaries; relevant methods may therefore have been missed. The same allocation questions could be used for routine duties such as access review, although this reporting example does not establish their usefulness there. A set of HCCM records does not establish complete NIS2 compliance. Cross-sector use requires checking the relevant legal, technical and safety conditions. Neither practical benefit nor an advantage over existing methods has yet been demonstrated. The planned cases will examine method use and specification quality; operational effects require separate testing.

## CONCLUSION

STRNIS2 provides a procedure for assigning cybersecurity work and recording the reasons for that assignment. Its reporting example shows why information cannot simply be removed from a form: someone must still obtain it when it is needed.

The allocation rule and HCCM make this responsibility explicit and give reviewers grounds to question an impractical arrangement. The next stage will examine whether practitioners can use the method with reasonable effort and produce correct, workable task specifications.

## ACKNOWLEDGMENT

This work forms part of the first author's doctoral research, supported by the University of Latvia, the Foundation for Public Participation and LLC Stratex.

## AI ASSISTANCE

AI-assisted tools, including ChatGPT, supported source discovery, critical review and editorial revision. The authors retain responsibility for the analysis, verification of sources and final manuscript.

## REFERENCES

- Beautement, A., Becker, I., Parkin, S., Krol, K. and Sasse, M. A. (2016). Productive Security: A Scalable Methodology for Analysing Employee Security Behaviours. Twelfth Symposium on Usable Privacy and Security, pp. 253-270. USENIX Association.
- Breidaks, I., Kalkis, H. and Semenov, A. (2026). Cognitive Load and Compliance: A Human-Centric Framework for NIS2 in Latvian SMEs. *Human Factors in Cybersecurity*, 208, pp. 11-20. doi:10.54941/ahfe1007408.
- Cabinet of Ministers (2025). Minimālās kiberdrošības prasības [Minimum Cybersecurity Requirements]. Regulation No. 397, adopted 25 June 2025. <https://likumi.lv/ta/id/361481> (accessed 5 September 2026).
- Calvo-Manzano, J. A., San Feliu, T., Herranz, Á., Mariño, J., Fredlund, L.-Å. and Moreno, A. M. (2025). CyberESP: An Integrated Cybersecurity Framework for SMEs. *Journal of Software: Evolution and Process*, 37(9), e70050. doi:10.1002/smr.70050.
- Chidukwani, A., Zander, S. and Koutsakis, P. (2026). Beyond self-reporting: Uncovering the operational realities of SME cybersecurity through expert assessment. *Computers & Security*, 164, 104839. doi:10.1016/j.cose.2026.104839.
- Desolda, G., Greco, F., Lanzilotti, R. and Tucci, C. (2026). MORPHEUS: A Multidimensional Framework for Modeling, Measuring, and Mitigating Human Factors in Cybersecurity. *ACM Transactions on Computer-Human Interaction*. Advance online publication. doi:10.1145/3829371.
- European Parliament and Council (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. *Official Journal of the European Union*, L 333, pp. 80-152. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> (accessed 5 September 2026).
- Hart, S. G. (2006). NASA-Task Load Index (NASA-TLX); 20 Years Later. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 50(9), pp. 904-908. doi:10.1177/154193120605000909.
- Hielscher, J., Schöps, M., Menges, U., Gutfleisch, M., Helbling, M. and Sasse, M. A. (2023). Lacking the Tools and Support to Fix Friction: Results from an Interview Study with Security Managers. Nineteenth Symposium on Usable Privacy and Security, pp. 131-150. USENIX Association.
- Holden, R. J., Carayon, P., Gurses, A. P., Hoonakker, P., Hundt, A. S., Ozok, A. A. and Rivera-Rodriguez, A. J. (2013). SEIPS 2.0: A human factors framework for studying and improving the work of healthcare professionals and patients. *Ergonomics*, 56(11), pp. 1669-1686. doi:10.1080/00140139.2013.838643.

- Imran, H., Turner, C., Nassar, S., Tran, Y. and Salama, M. (2026). Human-centered cybersecurity risk management for IT/OT-converged oil and gas operating facilities. *Computers & Security*, 167, 104918. doi:10.1016/j.cose.2026.104918.
- Kiran, U., Khan, N. F., Murtaza, H., Farooq, A. and Pirkkalainen, H. (2025). Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory. *Computers & Security*, 149, 104204. doi:10.1016/j.cose.2024.104204.
- Michalek, J., O'Shaughnessy, P. K. and Wahlstrom, K. (2026). Cyber incident prevention and response for small and medium sized enterprises: A scoping review. *Computers & Security*, 169, 104972. doi:10.1016/j.cose.2026.104972.
- Mullins, A. and Thompson, N. (2026). Technostress and information security - A review and research agenda of security-related stress. *Computers & Security*, 161, 104776. doi:10.1016/j.cose.2025.104776.
- Nelson, A., Rekhi, S., Souppaya, M. and Scarfone, K. (2025). Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST SP 800-61 Rev. 3. doi:10.6028/NIST.SP.800-61r3.
- Saeima (2024). Nacionālās kiberdrošības likums [National Cybersecurity Law]. Adopted 20 June 2024; consolidated text applicable on 5 September 2026. <https://likumi.lv/ta/id/353390> (accessed 5 September 2026).
- Venable, J., Pries-Heje, J. and Baskerville, R. (2016). FEDS: a Framework for Evaluation in Design Science Research. *European Journal of Information Systems*, 25(1), pp. 77-89. doi:10.1057/ejis.2014.36.
- Vidal, N., Moradpoor, N. and Maglaras, L. (2025). Everyone Needs AIR: An Agnostic Incident Reporting Framework for Cybersecurity in Operational Technology. *arXiv preprint 2510.20858*. doi:10.48550/arXiv.2510.20858.