NVE

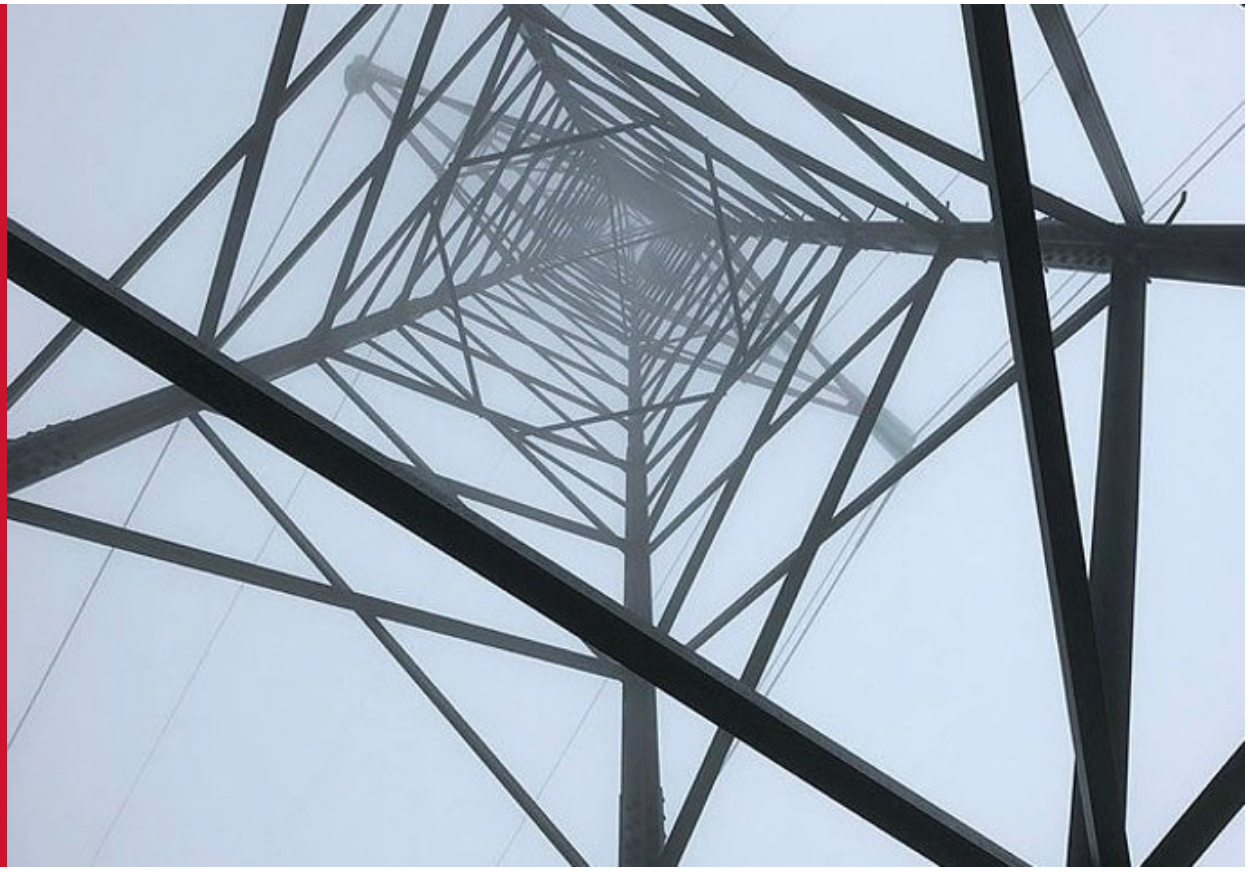
RAPPORT

Nr. 2/2020

ICT security in procurements and outsourcing in the Norwegian hydroelectric power sector

- Checklist

Maren Maal, Katrine Krogedal og Arthur Gjengstø



Rapport nr. 2/2020
ICT security in procurements and outsourcing in the Norwegian hydroelectric power sector

Published by: Norges vassdrags- og energidirektorat

Editor: Janne Hagen

Author(s): Maren Maal, Katrine Krogedal og Arthur Gjengstø

Printing: NVEs hustrykkeri
Forsidefoto: Bjørn Lytskjold, NVE
ISBN: 978-82-410-1981-4
ISSN: 1501-2832

Summary: This report presents a check list for ICT Security in procurement- and outsourcing processes. The checklist builds on the Norwegian Energy Act and regulation, in addition to guidelines from the Norwegian National Security Authority (NSM) and best practices. It covers the full life cycle of an agreement.

Keywords: ICT Security, Procurement

Norwegian water resources
and energy directorate (NVE)
Middelthunsgate 29
P.O. box 5091 Majorstua
0301 OSLO, Norway

Telephone: +47 22 95 95 95
Email: nve@nve.no
Internet: www.nve.no

08 January 2020

Foreword

Norwegian hydroelectric power plants and grid companies are transforming and modernizing their operations towards increased digitalization. In this context, supply chain security is challenging, due to lack of control and transparency along complex chains of interlinked collaborating vendors.

It is well known that many companies do not have enough resources to handle serious unwanted digital events by themselves and depend on good collaboration with vendors also in digital emergencies. Good digital emergency preparedness can however be formed early in a procurement process, and the topic should be addressed before contract negotiation and signing.

In 2019, Price Waterhouse Coopers (PWC) was engaged by the Norwegian Water Resources and Energy Directorate (NVE) in order to develop an ICT-security checklist for procurement and outsourcing. The checklist builds on the Norwegian Energy Act and regulation (kraftberedskapsforskriften), in addition to guidelines from the Norwegian National Security Authority (NSM) and best practices. It covers the full life cycle of a business relationship. The English version of the checklist is documented in this report.

We thank everyone that has contributed to the checklist and hope that the checklist will be a useful tool for the hydroelectric power industry in Norway and its vendors in ongoing and future procurement- and outsourcing processes.

Oslo, 08.01.2020

Ingunn Åsgard Bendiksen

Director

Department of Emergency and Contingency Planning

2019

A cybersecurity checklist for procurement and outsourcing in the energy sector

Introduction

The digital transformation of the energy supply sector is accompanied by an evolving landscape of risks. As the value of digital infrastructure increases, so does the consequences of interruption of services, manipulation of data, and immobilization of information systems. Furthermore, the control over systems and services is hampered by the proliferation of sub-contractors and externally developed services, meaning it is crucial for companies to enforce stringent security requirements in their procurement processes. Finally, the energy sector is being increasingly targeted by cyber attacks. All of the above makes the securing of information systems a critical component in the quest for holistic and efficient security management, including the security of energy sensitive information and brick and mortar facilities. In order to guide and support these efforts, PwC has developed a check list containing guiding ICT requirements relevant for procurement and outsourcing in the energy sector. The requirements are derived from the Norwegian Energy Act (Energiloven 2019) and energy emergency preparedness regulations (kraftberedskapsforskriften 2018), as well as general best practice and guidelines from the Norwegian National Security Authority (NSM) and reports from the Norwegian Water Resources and Energy Directorate. In addition, PwC has conducted interviews with relevant actors in order to obtain their insights and feedback. Quality control has been performed by PwC subject matter experts.

This is a general check list. In order to satisfy security needs, users of this tool need to assess the ways in which the nature of their organisation (e.g. size, location) and business context affects their specific needs and requirements. Furthermore, despite its comprehensiveness, the list is not exhaustive in terms of all the security requirements an organisation needs to consider.

Key terms:

- **Information security** entails ensuring the confidentiality, integrity and accessibility of information assets. In order to safeguard satisfactory information security, organisations have to prioritise technical security measures as well as human and organisational/governance factors.
- **Outsourcing** refers to the external distribution of central operations, such as application operations/management and system development. The terms outsourcing, sub-contracting and competitive tendering are used interchangeably.
- **Procurement** is taken to mean the ordering and/or acquisition of goods or services. There are several categories of procurement. The acquisition of management control systems monitoring and controlling important production facilities and networks, or other systems storing/handling sensitive energy information, will trigger more stringent requirements than a system or service handling non-sensitive information.

The security requirements of the organisation and its sub-contractors will depend on (1) the type of procurement/outsourcing; (2) whether/to what extent sensitive energy information is handled; and (3) the classification (class 1, 2 or 3) of the system or facility in question.

Phase 1: Preparation

In order to ensure the quality of final deliveries, the initial phase of the procurement process requires special attention. It is in this phase that the detailed preconditions of the outsourcing and procurements are developed, which might include key specifications related to security and preparedness. In order to attain the appropriate level of security, the organisation needs to assess the ways in which the outsourced/procured service will be integrated with existing ICT systems.

Risk assessment of outsourcing and procurement

- ❑ We have documented a risk assessment of the outsourcing/procurement.
- ❑ We have presented/discussed the outsourcing/procurement and its related risk assessment with high level management.

Evaluation of capabilities, preconditions and the relevant business context

- ❑ We have a clear overview of the most important business processes and flows of information that could be affected by the outsourcing/procurement.
- ❑ We possess the necessary level of competency to specify the relevant requirements to sub-contractors (with regards to security, integration, procurement, internal business processes and legal)
  - ❑ If no; we have access to this competency through other means (e.g. consultants or cooperation with peers)
- ❑ We understand what type of outsourcing/procurement we are acquiring, as well as its related security requirements and challenges.
- ❑ We have reviewed the whole process of outsourcing/procurement, and assessed whether the organisation is able to fulfil security requirements in all phases (planning, acquiring, implementing, managing and terminating).

Compliance

- ❑ We are aware of the relevant legal requirements and regulations related to outsourcing/procurement, both in Norway and internationally.
- ❑ We have mapped out and documented all internal security and preparedness requirements related to the outsourcing/procurement in question.
- ❑ We have developed requirement specifications for security, including requirements that become relevant if further security measures are to be implemented.
- ❑ We have assessed whether the outsourcing/procurement will be a central part of our digital preparedness and the management of critical systems containing sensitive energy data.

Decision-making related to outsourcing and procurement

- ❑ We have involved top level management in the decision to outsource/procure, and in decisions to change related contracts.
- ❑ Our line manager has ensured that the outsourcing/procurement and the sub-contractor model is verified by top level management.
- ❑ We can verify that the outsourcing/procurement ensures a level of security and preparedness that is better or on par with the existing solution.

Phase 2: Procurement

Based on the assessments and specifications of requirements in the preparatory phase, the organisation should be able to evaluate the quality of the offers received in the procurement phase.

Risk assessment in the procurement phase

The organisation's assessment of relevant risks will affect the selection of security requirements. In addition, the organisation should assess the need and opportunity for conducting a limited tender competition with a pre-qualification phase.

- ❑ We have ensured that the team involved in the outsourcing/procurement process is able to assess risks based on key competencies in security, integration, internal management processes and legal matters.
- ❑ We have evaluated the need for performing a country risk assessment[1] in the cases where the outsourcing/procurement is tied to territories outside the EU/EEA, and in other cases where such assessments are deemed necessary.
- ❑ We have made sure to share a minimum of sensitive data about the organization in our tender documents.
- ❑ In the cases where the outsourcing/procurement involves sensitive energy data, we have assessed the need for restricted tendering.
- ❑ We have safeguarded tender documentation sufficiently.
- ❑ In cases where the supplier is unable to satisfy the security-related requirements, we have assessed the need for an additional risk assessment and identification of risk reducing measures.
- ❑ When subject to the Security Act: We have assessed the need for identifying the supporting/critical objects and infrastructure relevant for our outsourcing/procurement.

It is essential that the contract in use sets out clear ICT security requirements and responsibilities for the supplier. Unequivocal procedures for verification and audit of contractual requirements should be in place before the contract is signed and the outsourcing/procurement is materialised.

Requirements for the supplier prior to the tender process

- ❑ We have informed the supplier that all information and data are the properties of our organisation, and that they are to be treated securely and in accordance with relevant laws and best practices. Furthermore, we have informed suppliers that the data cannot be re-shared without our consent.
- ❑ We have evaluated the need for an information security agreement with suppliers in cases where the procurement process involves sharing of sensitive energy data.
- ❑ We have requirements in place ensuring suppliers follow all relevant provisions set out in the Energy Emergency Preparedness regulation (kraftberedskapsforskriften - KBF).
- ❑ We have set a requirement for the establishment of a security contract, as well as requirements ensuring that supplier personnel with access to sensitive information sign non-disclosure agreements (NDA)s and are made aware of all security requirements.
- ❑ We have put in place appropriate requirements for uptime and system reliability.

[1] See *Geografisk risiko – oversikt over listeførte land* at finanstilsynet.no.

- ❑ We have set requirements for remediation in cases of discrepancies/breach related to the defined outsourcing/procurement requirements.
- ❑ We have assessed the need for access to critical personnel and resources, including equipment and reserve materials, in extraordinary situations.
- ❑ We have set requirements for the detection, notification and handling of the supplier's security-related events.
- ❑ We have set requirements for exit strategies which include the return/relocation/deletion of our information in cases where this is deemed necessary, for example when a supplier is acquired by a third party, declares bankruptcy, or if the service changes. The contract in place needs to specify practical and financial matters.

Security requirements

- ❑ We have set requirements for the supplier to provide independent audit reports, or alternatively that we ourselves perform security audits.
- ❑ We have set requirements for our ability to review the security measures implemented by the supplier for ensuring the security of our information at rest and in transit.
- ❑ We have set requirements for the supplier to perform background checks[2] of personnel before employment. The supplier is required to have access control and activity logging. This is particularly important when sensitive energy data is involved.
- ❑ We have informed the supplier that our access control is based on need-to-know and is time limited.
- ❑ The supplier knows the extent of their access to our information (i.e. who knows what), as well as how this information should be handled, stored, and segregated from other clients' data.
- ❑ We have set requirements for the supplier to inform us about organisational changes and changes in their use of sub-contractors.
- ❑ We have set requirements for the supplier to put in place backup solutions.
- ❑ Based on the relevant threat landscape and threat actors, the supplier performs sufficient security monitoring with the ability to uncover potentially damaging events and doings.
- ❑ The supplier has routines for security event management and reporting of security incidents and discrepancies.
  - ❑ If yes: We have set requirements for the supplier to log security events, as well as to report and communicate any discrepancies.
- ❑ The supplier has agreed to coordinate and cooperate in the effort to develop and test emergency preparedness routines.
- ❑ The supplier has put in place procedures for the approval of sub-contractors.
- ❑ The supplier has developed security improvement plans in order to be aligned with technological development and changes in the threat landscape.

Tender requirements

- ❑ We have developed clear tender requirements outlining delivery expectation (e.g. service/product quality, uptime, price, security and preparedness.)
- ❑ We have assessed the necessary duration of the outsourcing/procurement, keeping in mind that risks related to change increase over time.

[2] See document *Foreløpig tilleggsveileder til kraftberedskapsforskriften (2018),* NVE og *Sikkerhet ved ansattelsesforhold, -før, under og ved avvikling (2017),* The Norwegian Policy Security Service et al.

- ❑ We have barred suppliers from using our information/data to improve their own services (or for other purposes) without our consent.

Evaluation and selection of supplier
It can be beneficial to establish an internal project whereby the organisation involves employees with relevant competencies (e.g. systems, procurement, legal, ICT, security, emergency preparedness etc.). This ensures comprehensive quality assurance and organisational involvement.

- ❑ Based on open source intelligence we have performed background checks of the supplier and its key personnel. We have contacted references and acquired any available information ensuring the supplier is a legitimate actor.
- ❑ We have assembled a team with the necessary competencies within security, integration, procurement, internal business processes and legal matters. This team assesses the suppliers and their respective bids.
- ❑ We have examined whether the suppliers have established management systems for information security and whether they retain certifications based on international standards (e.g. ISO/IEC 27001:2017).
- ❑ For cloud suppliers: We have examined whether the suppliers are compliance with international standards (e.g. ISO 27018/27017).

Contract negotiations
- ❑ We have reviewed the whole life cycle of the outsourcing/procurement with the supplier.
- ❑ We have ensured our right to compensation and contract termination in the event of the supplier experiencing and/or mishandling major security incidents.
- ❑ We have ensured our right to contract termination in the event of changes in ownership, downsizing or other changes that may have an effect on the supplier's ability to deliver the service/product.
- ❑ We have clearly defined the distribution of responsibilities in the contract with the supplier, including responsibilities tied to the update of software and requirements related to update and incident notifications.
- ❑ We have placed upon the supplier a duty to transfer knowledge/competency to new suppliers when the contract ends.
- ❑ For cloud suppliers: We have assessed whether the supplier's standard requirements and terms can be integrated in the contract.
- ❑ The contract ensures that we have access to the necessary training related to the product/service, and that support from the supplier is available throughout the lifecycle of the delivery, including in termination phase.

Phase 3: Implementation and management

This phase describes the implementation, integration and management of the service that is being outsourced/procured. Best practice is to establish routines for the continuous follow-up of suppliers. This is important for the detection and handling of potential discrepancies from the delivery requirements.

Supplier relations, control and audit

- ❑ We possess the necessary competencies and resources to ensure a sound supplier relationship and efficient communications.
- ❑ We have requested information about access lists to systems and physical spaces in order to ensure the continuous review of access controls.
- ❑ We have received access to discrepancy logs in order to ensure that the supplier follows procedures for notification, reporting and evaluation in relation to security incidents and downtime beyond critical thresholds.
- ❑ We have received access and sufficient explanations regarding the findings of supplier third party audit reports.
- ❑ We have received access to documentation of emergency preparedness exercises related to the service being outsourced/procured.
- ❑ We have received access to documentation confirming that the supplier is operating in accordance with KBF.
- ❑ We have received access to documentation related to supplier risk assessments and accompanying remediation plans.
- ❑ We have audited the risks relating to the outsourcing/procurement. This may be a yearly affirmation from the supplier stating that they are in accordance with KBF.
- ❑ We have audited the supplier.
- ❑ We have revised the supplier's emergency backup solutions.
- ❑ We have revised the supplier's security training program for employees with a role tied to our outsourcing/procurement contract.

Continuous risk management and quality assurance

- ❑ We have reviewed changes in national and international requirements and guidelines.
- ❑ We have assessed whether and how changes in our organisation generates adjusted requirements for the supplier.
- ❑ We have assessed how new requirements for ICT security may change as a consequence of changes in ownership both in our organisation and on part of the supplier.

Phase 4: Termination

The termination phase is the phase where the affiliation with the client seizes and the contract ends. There can be several reasons behind the termination of a contract, such as an unsuccessful bid, the breach of a contract, bankruptcy or changing circumstances on the part of the supplier (or its location) that are deemed unacceptable.

- ❑ We possess the necessary competencies (i.e. security, integration, procurement, internal business processes and legal matters) for the safeguarding of our interests, including those related to security.
- ❑ We have ensured the transfer of knowledge/competency from the outgoing supplier to the new supplier, and have done so contractually.
- ❑ We have initiated a plan for the restoration of the service in our organisation, or for its transfer to a new supplier (alternatively through in-sourcing).
- ❑ We have initiated a plan for the responsible destruction of data in the possession of the outgoing supplier.
- ❑ We have assessed the need for additional logging and monitoring of access controls during the termination phase.
- ❑ We have assessed the need for limited access control during the termination phase.

Bibliography:

- *Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften), (2014).*
- *Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (Energiloven), (2019).*
- Nasjonal sikkerhetsmyndighet, *NSMs Grunnprinsipper for IKT-sikkerhet*, *(2018).*
- Nasjonal sikkerhetsmyndighet, *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting,* (2018).
- Norges vassdrags- og energidirektorat, *Regulering av IKT-sikkerhet* (2017).
- Norges vassdrags- og energidirektorat, *IKT-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen* (2018).
- Norges vassdrags- og energidirektorat, *Spørsmål ved revisjon: Informasjonssikkerhet - kapittel 6* (2019).
- Norges vassdrags- og energidirektorat, *NVEs Generelle betingelser for kjøp av tjenester.*

Recommended literature and standards:

- *Forskrift om IT-standarder i offentlig forvaltning, (2013).*
- *Lov om nasjonal sikkerhet (sikkerhetsloven), (2019).*
- *Lov om offentlig anskaffelser (anskaffelsesforskriften), (2016).*
- International Organization for Standardization (ISO), *International Standards*
    - *ISO 27001*
    - *ISO 27002*
    - *ISO 27018*
- International Electrotechnical Commission (IEC), *International Standards.*
    - *2017*
- Difi*, Standard modell for anskaffelsesprosessen, (2019).*
- Difi, *Elektronisk handelsformat (EHF), (2019).*
- North American Electric Reliability Corporation (NERC), *Critical Infrastructure Protection Standards (CIP).*
- *National Institute of Standards and Technology (NIST), 800-Series.*
- Energy Sector Control Systems Working Group (ESCSWG), *Cybersecurity Procurement Language for Energy Delivery Systems (2014).*

The following organisations have contributed to this check list:

- Energi Norge
- KraftCERT
- Distriktsenergi
- Hafslund Nett
- Nettalliansen

NVE

Norges vassdrags- og energidirektorat

MIDDELTHUNSGATE 29
POSTBOKS 5091 MAJORSTUEN
0301 OSLO
TELEFON: (+47) 22 95 95 95

www.nve.no