Risk and control objectives over non-discriminatory controls in the Norwegian broadband market

January 2022

Nasjonal kommunikasjons-myndighet

pwc

PwCs Third Party Assessment for Nkom – Phase 2
Version 1.0

Disclaimer

This report has been prepared solely for Norwegian Communications Authority's use with the purpose set out in The Contract dated 2021-09-30.

Description of the engagement

PwC was engaged by the Norwegian Communications Authority (hereby referred to as "*Nkom*") to develop a detailed risk and control matrix to be used in a public hearing scheduled Q1 2022. The current phase includes detailing the risk and control objectives that are relevant to Telenor's non-discrimination obligations. This will form the basis of the third party attestation which will be developed by Telenor. The scope of the related control activities will be determined by Telenor after Phase 2 completion. The estimated time frame for this phase of the engagement is from October 2021 to March 2022. The background for this engagement is outlined in the following slides.

Our assessment is based on interviews conducted with Nkom, Telenor and central access seekers in the Norwegian broadband market. Information supplied by Nkom, Telenor and central access seekers has not been independently verified by PricewaterhouseCoopers (PwC) and we therefore do not provide any assurance as to its completeness or accuracy. PwC has not performed any quality assurance or controls of Telenor's business processes.

Nkom is entitled to use information from this report within their business, in accordance with The Contract. PwC does not accept any responsibility for losses suffered by Nkom or others as a result of the distribution, reproduction or use of our final or draft report contrary to the specified conditions or engagement letter. When sharing the report, partly or in its entire form, Nkom ensures that any disclaimer PwC has included or later wishes to include in the report is reproduced in its entirety in all copies shared. PwC holds the property rights to their own tools and methodological basis. Any actions based on the report are made on the person's own responsibility.

pwc

Contents

Executive summary

Background

Nkom issued a letter in June 2020 regarding Telenor's non-discrimination obligations. A concern was raised that the current non-discrimination requirement based on Equivalence of Output (EoO) has not worked effectively.

Nkom decided that an external third party assessment of Telenor's non-discriminatory controls should be performed to demonstrate their compliance. Controls will be based on the matrix of risks and control objectives outlined in this report.

Approach

PwC's approach includes document review and process walkthroughs with Telenor, Nkom and central access seekers in the Norwegian broadband market. This resulted in the identification of related risks and the definition of control objectives, which have been anchored with Nkom throughout the process. The final result is included in Chapter 3 (Risk and control matrix), and is planned to be presented to related stakeholders through a public hearing. The results from the hearing will be incorporated into the final risk and control matrix, which will be used as a basis for the third party attestation of Telenor's non-discriminatory controls.

Summary

Through this project PwC have identified 44 unique risks, and 83 unique control objectives. These cover 8 central areas that are considered critical for Telenor's ability to have a well-functioning internal control environment that ensures their non-discrimination obligations.

After the public hearing, feedback will be incorporated into the risk and control matrix when creating their third party attestation scoping. The objective of the attestation is to have an independent third party to verify how Telenor adheres to their non-discrimination obligations.

The 8 central areas with identified risks and related control objective include:

- Entity Level
- Coverage information prior to order
- Order and delivery
- Fault repair
- Monitoring of KPI
- Monitoring of SLA/SLG
- Test and Diagnosis
- IT General Controls (ITGC)

01 Background and scope

Background and scope

Background for the engagement

Telenor is an incumbent telecom provider with significant market power* in the Norwegian broadband market as defined by the market (3a/3b) decision issued by Nkom December 2018. Objections to Telenor's non-compliance with their non-discrimination obligations was issued by an access seeker [1]**, which triggered Nkom to issue a letter in June 2020 regarding Telenor's non-discrimination obligations. It was assessed that the current non-discrimination requirement based on Equivalence of Output (EoO) has not worked effectively according to the Electronic Communications Act (§ 4-7).

An external third party assessment was, in Nkom's assessment, an appropriate measure to ascertain whether the non-discrimination obligations based on EoO works sufficiently. Nkom has an ambition of increasing trust, openness and transparency with regards to Telenor's non-discriminatory practices and internal controls. To achieve this, Nkom has decided that Telenor shall demonstrate their compliance through a third party assessment of their non-discriminatory controls. An important aspect related to the assessment is whether and how Telenor's systems and processes ensure non-discriminatory functionality, reliability, quality and performance between wholesale customers and Telenor's own business.

Scope of the engagement

PwC was engaged by Nkom to develop a risk and control matrix to be used in a public hearing scheduled for the first quarter of 2022. This report is set to identify and detail applicable risks and control objectives that are relevant for Telenor's actual or potential anti-competitive behavior in the Norwegian broadband market. The matrix will form the basis of a third party attestation with the objective of verifying whether Telenor adhere to their non-discrimination obligations.

In the following sections, we will elaborate on the expectations for Telenor's follow-up of the developed risk and control matrix, which will culminate in the above-mentioned third party attestation.

*

Provider with significant market power
Telenor ASA was defined as a provider with significant market power pursuant to the Norwegian Electronic Communications Act (ekomloven) § 3-3. In Nkom's Market 3a and Market 3b decisions (20.12.2018), a number of special obligations are imposed, including the obligation to provide access to the regulated products on non-discriminatory terms.

**

Complaint from access seeker
The access seeker, Global Connect, claimed in October 2019 that Telenor were in breach of several non-discrimination obligations. Non-compliance allegations included discrimination in terms of reduced delivery and fault correction for the access seeker compared to Telenor's own end-user business [1].

[1] Nkom has issued a correction order and an administrative fine in the case, both of which have been appealed

Expectations and next steps (1/2)

Expectations for Telenor

Nkom has an expectation that Telenor will map its control activities to the risks and control objectives documented as part of this engagement. These control activities will subsequently be tested by an independent third party and be presented in a recognized third party attestation standard, such as ISAE 3000*.Telenor's control activities should demonstrate how the risks are mitigated and how control objectives are addressed through their internal control activities.

Further, it is an expectation from Nkom that Telenor performs an equivalence test to verify that the key systems provides equivalent functionality and access to information. The assessment should be executed by an independent and objective party outside Telenor Group. The equivalence test should be performed as reperformance, desktop review and/or documentation verification to ensure verification of equivalence.
It is an expectation that Nkom will get full assurance over these areas through an ISAE 3000. Yet, if timing and circumstances doesn't allow for this, Telenor should find appropriate alternatives. For an indicative timeline regarding the upcoming phases and timing targets, please see below.

1 — Risk and control matrix out on Public Hearing

Jan - Feb 2022

Key tasks:
- Public hearing sent out first quarter 2022
- Interested stakeholders are encouraged to provide input and opinions on matters to be included, excluded or adjusted in the risk and control matrix

2 — Final risk and control matrix approved by Nkom

Feb- Mar 2022

Key tasks:
- Incorporate input/feedback from stakeholders following the public hearing
- Final version of the risk and control matrix to be approved by Nkom

3 — Telenor to confirm control activities to address risk and control matrix

Mar - May 2022

Key tasks:
- Telenor to develop and map control activities to identified risks and control objectives in the risk and control matrix
- Telenor to assess if there is a need to engage external expertise to assist in the mapping and establishing of control activities

4 — Nkom to approve Telenor's controls

May- June 2022

Key tasks:
- Dialogue with Nkom about the developed control activities
- Nkom to ultimately approve Telenor's selected control activities to be tested as part of the forthcoming third party attestation

5 — Telenor to obtain an ISAE 3000 third party attestation

June - Des 2022

Key tasks:
- Telenor to engage a third party to carry out the third party attestation
- Telenor to present the attestation report to Nkom and other significant stakeholders upon its completion

***ISAE 3000 Report**

Is a third party assessment of processes and controls, with intended use by a service organisation to demonstrate their internal controls related to a specific subject. e.g. non-discrimination.
An ISAE 3000 attestation can be either Type I or Type II:

- Type I: provides assurance on the suitability of design and existence of controls
- Type II: provides assurance on suitability of design, existence and operational effectiveness

In other words, a Type II is over a period of time and tests operational effectiveness. Type I takes a snapshot of whether the control design is sufficient to address the control objectives.

Expectations and next steps (2/2)

Example of control activities to be developed for a third party attestation

A third party attestation report includes control testing performed by a third party. The controls to be tested are defined by the risks related to the scope of the report. Whereas a control objective describes how the organisation mitigates the risk, the control activity describes the control(s) the organisation have implemented to meet the control objective. An example of the dynamic between a risk, a control objective and the control activity is illustrated below.

This phase of the project has included the identification of risks and defining control objectives. Telenor will be responsible for defining the control activities that they have implemented and/or plan to implement to meet the control objective. Nkom will confirm that Telenor's control activities sufficiently cover the control objectives before next phase of the project commence.

Note that potential deviations noted on control activities in the future independent auditor report does not necessarily constitute non-compliance with Telenor's non-discrimination obligations. An identified deviation would rather indicate that internal control activities set up to ensure compliance with their obligations are not working effectively. Thus the risk of non-compliance is not properly mitigated.

EXAMPLE:

Risk	Control Objective	Control Activity
Access is granted to individuals without a business need for such rights	*A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services, including terminated users*	*Procedures exist that define the process for provisioning and removing IT access.*
		User account requests for new and modified users require authorised manager approval.
		Employee exit procedures including the removal of IT access are completed for terminated users
		User accounts and access rights for retired employees and leavers are promptly removed

02 Methodology and approach

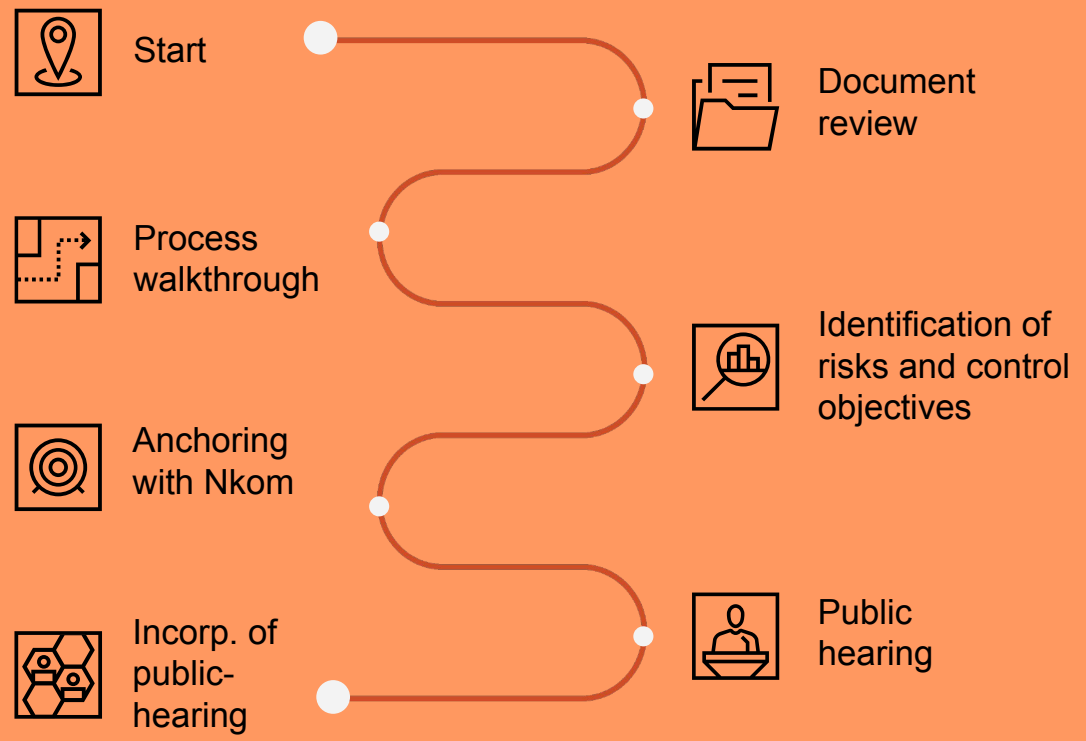
Methodology and approach

Methodology

The suggested risks and control objectives are identified and outlined based on PwC's internal methodology, the team's professional judgement, best practice, and external methods and frameworks. These include, but are not limited to;

- *Inspection* and *review* of documentation issued by Nkom, studies on how non-discrimination is followed up in similar markets, and documentation of internal systems and processes issued by Telenor
- *Observation* of and *enquiry* with key stakeholders both internally within Telenor and externally with central access seekers
    - Internal enquiries included walkthroughs in high risk areas on both entity, process, system interface and data integrity level
    - External enquiry with central access seekers on their subjective experience of current processes and potential and actual non-discrimination risks
- Application of best practice from internal control frameworks such as COSO and PwC's internal and external audit methodology for designing, implementing and evaluating an organisation's internal control

Approach



03 Risk and control matrix

Risk and control matrix

What is a risk and control matrix

The risk and control matrix is a framework which can help an organisation identify, rank, and implement control measures to mitigate risks. The framework is a repository of risks that pose a threat to an organisation's operations, as well as the control objectives in place to mitigate those risks. To be able to develop such a framework, an understanding of the organisation's risk profile is vital. Based on the understanding of the relevant risks, control objectives are formulated to align future control activities with the mission. In this instance, the mission is to ensure Telenor's compliance with their non-discrimination obligations.

The next slide introduces the breakdown of identified risks and related control objectives into a selection of specific topics;

- Entity Level
- Fault repair
- Test and Diagnosis
- Coverage information prior to order
- Monitoring of KPI
- IT General Controls (ITGC)
- Order and delivery
- Monitoring of SLA/SLG

The intended use of the risk and control matrix

The risk and control matrix will provide Telenor with the foundation for their mapping of control activities. The addition of their control activities to the risk and control matrix will provide a comprehensive risk and control framework. This will complement their compliance efforts with regards to their non-discrimination obligations and provide assurance over the completeness of their efforts. Telenor's documented control activities, along with the risks and control objectives, will provide the basis for a future third party attestation report. The scope of the independent attestation report will be to assess design and (subsequently) the operating effectiveness of the control activities. This will provide Telenor with the opportunity to objectively demonstrate their adherence to their non-discrimination obligations.

Part of the reasoning for utilising such a framework for this project is that the structure of the framework makes it highly adaptable. This can be useful in case it is of interest to apply a similar framework for other regulated entities, such as regional fiber providers. This also provides Nkom the opportunity to reuse the framework for other objectives and/or entities by altering the entity specific or subject specific content. Lastly, it provides an internationally recognized trust and transparency framework which benefits both the producing and receiving parties.

Risk and control matrix

Rationale for the breakdown
The risk and control matrix is segmented into eight, logical groups. The groups include areas and processes identified as critical for Telenor's ability to meet their non-discrimination obligations and have a well-functioning internal control environment.

Entity level control objectives
Includes risks and controls which support Telenor's internal control environment. Following the COSO principles, this includes: risk assessment, control activities, information and communication and monitoring activities.

Coverage information prior to order
Focuses on access seekers receiving information of the same quality and timeliness as Telenor.

Order and delivery
Risks and controls relate to Telenor's monitoring of subcontractors and equal opportunity for access seekers to communicate with subcontractors.

Fault Repair
Risks and controls relate to non-discrimination during fault repair such as subcontractors favouring Telenor retail over access seekers.

Monitoring of KPIs
Monitoring of Key Performance Indicators relate to risks and controls to ensure the completeness, accuracy and follow-up of KPIs.

Monitoring of SLA/SLG
Monitoring of Service Level Agreement (SLA) and Service Level Guarantee (SLG) relate to risks and controls for Telenor's perceived incentive to reduce the quality of their copper services to accelerate the decommissioning of the network.

Operations (excl. fault repair)
Risks and controls refer to non-discrimination related to Telenor's test and diagnosis tool and communication with access seekers during incidents.

ITGC - Data and systems
IT General Controls (ITGCs) are necessary to ensure that measures and safeguards are put in place to protect the confidentiality, availability and integrity of Telenor's systems and data.

I. Entity level control risks and control objectives

Ref.	Risk	Control Objective
ELC.1	**Control environment** The tone at the top does not include clear directions for employees to ensure their non-discrimination obligations.	**a)** There has been established governing documents such as organisational strategy, policies and procedures that explicitly communicate employees' responsibilities to prevent non-compliance with the non-discrimination obligations.
		b) Management has secured the establishment of control mechanisms to detect any misconduct that may arise related to the non-discrimination obligations. Such mechanisms may include establishment of whistleblowing hotlines for staff to report misconduct.
		c) Management has secured the establishment of control mechanisms to ensure the organisation appropriately responds to any misconduct related to their non-discrimination obligations in the Norwegian broadband market.
		d) The organisation's leadership has an established strategy stating how to secure that all key systems and manual processes related to broadband services shall comply with the Equivalence of Outputs obligations.
		e) Management performs an annual review of governing documents related to their responsibilities to ensure non-discrimination.
		f) Management has effective mechanisms set up to ensure that policies and procedures are known and complied with in the organisation.
ELC. 2	**Risk assessment** Management fail to identify, analyse and mitigate risks. Organisation's lack of risk assessment result in the inability to identify non-compliance with the non-discrimination obligation.	**a)** Management regularly receives analysis of the identified risks related to non-compliance with the non-discrimination obligations. Based on likelihood and consequence of the identified risks, management assesses the need for risk management, and implements mitigating measures as needed.
		b) Management regularly decide on precautions based on risk assessments. Measures to eliminate or reduce the risk of actual and potential non-compliance are performed timely and documented accordingly.

I. Entity level control risks and control objectives

Ref.	Risk	Control Objective
ELC. 3	**Control activities** Management fails to select and develop control activities that contribute to the mitigation of non-compliance risk with the non-discrimination obligations to acceptable levels.	**a)** The organisation has control activities in place ensuring that access seekers have the equal opportunity to automate their processes as themselves. Any instances were the organisation has better opportunities and/or there is a risk of unequal opportunities are quickly identified and remediated.
ELC. 4	**Control activities** There are unfair barriers for access seekers that want to establish themselves as providers, Resulting in reduced probability of new access seekers entering the Norwegian broadband market.	**a)** The organisation regularly identify and assess barriers for access seekers to gain access to their wholesale products. Any identified risks and/or barriers are followed up and mitigating measures are implemented. **b)** The organisation has established clear guidelines for negotiations with prospective access seekers, and evaluate instances where request for negotiations do not lead to market entrance for confirmation that they did not restrict access to the market.
ELC. 5	**Control activities** The organisation has established high barriers to entry by having complex processes requiring extensive know-how and effort to establish a partnership with them. This results in reduced probability of new access seekers entering the Norwegian broadband market.	**a)** The organisation continuously assess how barriers for access seekers to gain access to their wholesale products can be decreased, and how their processes can be improved through input from access seekers on barrier complexity. Measures for improvement are regularly identified and implemented. **b)** Employees working with the organisation's access seekers have an independent management from employees working in retail, separate branding and office location including separate governance arrangements and separate incentive payments.
ELC. 6	**Information and communication** Management fail to communicate information regarding their responsibilities related to their non-discrimination obligations, resulting in a culture that favours internal deliveries over external deliveries.	**a)** There has been established a Code of Conduct and training program for staff to address compliance with the non-discrimination obligation, transparency, information sharing and confidentiality. **b)** The organisation regularly assess whether employees have sufficient awareness to ensure compliance with the organisation's obligation of non-discrimination, and any identified deficiencies are followed up in a timely manner.

I. Entity level controls risks and control objectives

Ref.	Risk	Control Objective
ELC. 7	**Information and communication** The organisation creates entry barriers by failing to sufficiently communicate the necessary information to support new partnerships in the Norwegian broadband market. This results in reduced probability of new access seekers entering the Norwegian broadband market.	**a)** The organisation actively support access seekers attempting to enter the Norwegian broadband market, ensuring that they have the necessary information to enter a partnership with them. Information include details such as planned technology changes and infrastructure roll-out etc.
ELC. 8	**Monitoring activities** Management fail to develop and perform evaluations to ascertain whether the organisation adhers to its non-discrimination obligations.This results in the inability by management to detect any non-compliance and initiate corrective efforts.	**a)** There has been established a body/group at senior level, with external, independent representation if deemed applicable, e.g. an Equality Access Board, with mandate and independence to ensure compliance with non-discrimination obligations. **b)** The organisation's leadership has established management review controls to ensure management are continuously monitoring compliance with their non-discrimination obligations. **c)** The organisation evaluate and communicate non-compliance deficiencies in a timely manner to the stakeholders responsible for taking corrective action(s), including senior management and BoD, as appropriate.
ELC. 9	**Monitoring activities** In case of emergency, i.e., during storm mode, the organisation's routines and processes favours retail above the access seekers, resulting in failure to uphold their non-discrimination obligation.	**a)** As part of the organisation's emergency preparedness, their routines and processes ensures compliance with the non-discrimination obligations by ensuring that access seekers are not disproportionally affected - neither in terms of service quality nor in terms of access to timely and sufficient information on the emergency. **b)** The organisation conducts ex-post analysis after cases of emergency to check compliance and issue guidance for similar events in the future.

II. Coverage information prior to order risks and control objectives

Ref.	Risk	Control Objective
PCIPTO. 1	The process for information regarding coverage prior to order does not have clear directions for the employees to sufficiently inform employees of their responsibilities related to the non-discrimination obligation.	**a)** Clearly defined policies and procedures are established for the manual operations related to coverage information prior to orders. The internal policies and procedures provide directions on the employees non-discrimination responsibilities. All employees are aware of their duties to non-discrimination.
PCIPTO. 2	Access seekers do not receive information of the same quality regarding coverage as retail.	**a)** The organisation ensures that access seekers receive information regarding coverage of the same quality as retail. The quality dimensions include completeness in terms of accessible lines, line characteristics, timeliness and interface functionality through coverage search and web based direct retail customer requests.
		b) The organisation periodically perform equivalence tests to ensure that the interface used to search for coverage information by access seekers are of the same quality and format as for retail.
PCIPTO. 3	Access seekers do not receive coverage information with the same timeliness as the incumbent provider's retail organisation.	**a)** The organisation regularly perform self assessments to evaluate whether data on new infrastructure deployment projects are communicated according to the timeliness obligations. i.e., data being available for access seekers and retail simultaneously without delay.

III. Order and delivery risks and control objectives

Ref.	Risk	Control Objective
POAD. 1	The process for order and delivery does not have clear directions for the employeess to sufficiently inform them of their non-discrimination responsibilities.	**a)** Clearly defined policies and procedures are established for the manual operations related to order and delivery. The internal policies and procedures provide directions on the employees non-discrimination responsibilities. All employees are aware of their duties to non-discrimination.
POAD. 2	Subcontractors favour retail deliveries over access seekers deliveries.	**a)** The organisation's contracts with subcontractors include requirements for non-discrimination between internal and external deliveries.
		b) The organisation requires that all subcontractors have internal controls to ensure non-discrimination between internal and external deliveries, and these are evaluated annually.
		c) The organisation monitors their use of subcontractors and has controls in place to identify and handle incidents in the delivery process where subcontractors could favour internal over external deliveries.
POAD. 3	Access seekers' lack of direct contact with subcontractors in relation to delivery can result in lower customer satisfaction than for retail.	**a)** Measures are in place to ensure communication with subcontractors are equally accessible to provide end users with updated relevant information regarding the delivery process.

IV. Operations risks and control objectives

Ref.	Risk	Control Objective
PO. 1	The process for test and diagnosis does not have clear directions for the employees to sufficiently inform them of their non-discrimination responsibilities.	**a)** Clearly defined policies and procedures are established for the manual operations related to test and diagnosis. The internal policies and procedures provide directions on the employees responsibilities related to the non-discrimination obligations accompanied by procedures which ensure all employees are aware of their non-discriminatory duties.
PO. 2	The system(s) used for testing does not provide the same level of quality for the retail as for access seekers.	**a)** The organisation ensures that the interface used for test and diagnosis for fiber and copper have the same level of quality for retail as for access seekers.
PO. 3	Access seekers do not have the same competence and prerequisites in the test and diagnosis tool as retail do to perform effective testing when standard broadband related faults emerge.	**a)** The organisation ensures that the access seekers using the test and diagnosis tool have the same level of competencies as retail do. Measures to secure fair prerequisite may include effective and equally accessible training material and support in using the tool
PO. 4	The organisation does not have a communication strategy on how to effectively communicate with access seekers to the wholesale broadband market when incidents occur.	**a)** A communication policy is established outlining how incidents are handled and communicated externally to access seekers.

V. Fault repair risks and control objectives

Ref.	Risk	Control Objective
PFR. 1	The organisation prioritises the fault repair for their own retail customers over those of access seekers.	**a)** Clearly defined policies and procedures are established for the manual operations related to fault repair. The internal policies and procedures provides directions on the employees responsibilities related to the non-discrimination obligations accompanied by procedures which ensure all employees are aware of their non-discriminatory duties.
PFR. 2	Subcontractors favour retail fault repairs over access seekers fault repairs.	**a)** The organisation's contracts with subcontractors include requirements for non-discrimination between internal and external fault repairs.
		b) The organisation requires that all subcontractors have internal controls to ensure non-discrimination between internal and external fault repairs, and these are evaluated annually.
		c) The organisation monitors their use of subcontractors and have controls in place to identify and handle incidents where subcontractors could favour fault repairs for retail over the access seekers.
PFR. 3	The organisation actively contacts the access seekers' customers when there are faults in their broadband services to incentivize them to become customers of our organisation instead.	**a)** Internal procedures for communication with customers is established ensuring that access seekers' customers are not incentivized to become customers of the organisation in conflict with non-discrimination obligations.
PFR. 4	Access seekers' lack of direct contact with subcontractors in relation to fault repair can result in lower customer satisfaction than for retail.	**a)** Measures are in place to ensure communication with subcontractors are equally accessible to provide end users with updated relevant information regarding the fault repair process.

VI. Monitoring of KPI/SLA risks and control objectives

Ref.	Risk	Control Objective
PMOKS.1	Monitoring and follow up of KPI reporting does not have clear directions for the employeess to sufficiently inform them of their responsibilities related to their non-discrimination obligation.	**a)** The process to prepare, monitor and follow up KPI reports have clearly defined policies and procedures. The internal policies and procedures provide directions on the employees responsibilities related to the non-discrimination obligations accompanied by procedures which ensure all employees are aware of their non-discriminatory duties.
PMOKS.2	The organisation's reported KPIs are not complete and accurate, including inaccurate definitions and carve-out of populations, making comparisons across retail and wholesale unreliable.	**a)** There have been established policies and procedures for the design of KPIs, including accurate definitions with product segmentation and any filtering of populations. Enabling comparisons of performance between retail and wholesale.
		b) The organisation ensures that the preparation of KPI reports is aligned with the framework established by relevant policies and procedures, including the definition of relevant populations for each KPI.
		c) The organisation's KPI methodology and reporting have incorporated quality checks of policies and procedures to ensure the integrity of the KPI reports.
		d) There has been established a policy and procedure for the change management of the KPI design, methodology and reporting.
		e) The organisation has processes to regularly verify that the KPI design and methodology is aligned with the evolution of access products and market reality, and to identify improvements in the reporting of KPIs. These processes include dialogue with access seekers and the NRA.
		f) They regularly evaluate the data generation process to validate the integrity of the process. This includes the data input, e.g deliveries and fault repairs, and the filtering of the data used in the generation of the KPIs.
		g) The organisation performs an independent review to audit the KPI process on a yearly basis to verify the integrity of the process and relevance of the established KPIs.

VI. Monitoring of KPI/SLA risks and control objectives

Ref.	Risk	Control Objective
PMOKS.3	Deviations between KPIs in retail and wholesale are not identified and/or not properly addressed.	**a)** In case of identified deviations, the KPI comparison of retail and wholesale includes documented qualitative and/or quantitative analysis. This can include analysis of deviation statistical significance, which will segment out following up of falsely identified deviations.
PMOKS.4	The KPIs, including the methodology, KPI design, and specification, is not openly available for relevant stakeholders in a timely manner. An updated design and specification of the organisation's reported KPIs, including the description of the product segmentation.	**a)** The organisation ensures that the updated KPI design and methodology is openly available for the supervisory authority and other relevant stakeholders. **b)** The organisation publish the KPIs on their website within 15 working days of the end of the reporting period.
PMOKS.5	Risk of manual data processing faults prior to KPI publishing, which can impact the accuracy and integrity of the KPIs. Impact being incorrect product segmentation and removal of irrelevant data points from the extracted delivery management system report (for copper and/or fiber).	**a)** The organisation has incorporated quality checks in the KPI publishing process to ensure identification of faults in the manual data processing prior to KPI publishing.
PMOKS.6	The reported KPIs are not aligned with the quality targets defined in the organisation's SLAs with the wholesale clients.	**a)** The organisation regularly reviews their KPI to confirm they are properly aligned with the SLA parameters in the wholesale SLAs.
PMOKS.7	Risk of the access seekers not having access to the correct underlying data related to delivery and fault repair of their respective lines. Resulting in reduced ability to compare the KPI performance against the organisation's reported KPIs.	**a)** The organisation has policies in place which confirms that access seekers will have access to the underlying data related to their own products on request or through monthly service reports.

VII. Monitoring of SLA/SLG risks and control objectives

Ref.	Risk	Control Objective
PSLASLG.1	The processes related to maintenance of Service Level Agreements (SLA) and Service Level Guarantees (SLG) do not have clear directions for the employees.	**a)** The organisation continuously monitor their wholesale performance compared to the targets of the SLAs, and have processes in place to ensure that any deviations are identified and addressed. The effectiveness of these measures are evaluated and improvements are incorporated into the process..
		b) Clearly defined policies and procedures are established for follow-up of SLG commitments.
PSLASLG.2	The incumbent operator reduces the quality of delivery related to copper based broadband services in order to push customers over to fiber or FWA based services.	**a)** The organisation has established controls to ensure the quality of the delivery related to copper based based broadband services. These are monitored and they have implemented measures for improvement where their services fails to meet the required level.
PSLASLG.3	The incumbent operator intentionally reduces the quality of fault repair for copper based broadband services to push customers over to fiber based services to accelerate the closure of the copper network.	**a)** The organisation ensures that the quality of fault repairs are of an equal standard regardless of the type of broadband service and that internal procedures are established ensuring fault repairs for both copper based and fiber based services are performed to the same standard.

VIII. Data/System risks and control objectives

Ref.	Risk	Control Objective
ITGC. 1	Management does not maintain a list of systems and dataflows sufficient to confirm its compliance obligations.	**a)** Management annually reviews and approves the scoping of key systems for broadband services provided to retail and to access seekers.
		b) Any significant changes to system architecture or key systems should undergo review for management to maintain necessary oversight of the non-discrimination aspects of system architecture and key systems.
		c) An up to date data and systems list, including a data flow list periodically undergo review by management for them to maintain necessary oversight of the non-discrimination aspects of system architecture and key systems.
ITGC. 2	Lack of defined system architecture and adequate system description demonstrating the interface dependencies for the systems used by retail and wholesale value chain (hereby referred to as "key systems") creates an overly complex system compilation that establishes high entry barriers for new access seekers in the Norwegian broadband market.	**a)** Management regularly reviews and approves the individual system descriptions, system architecture and its dependencies per relevant key system in scope.
ITGC. 3	Key systems in scope does not comply with the non-discrimination obligations of providing the same quality information in a timely manner with same functionality and opportunity for automation as retail.	**a)** An independent and objective assessment is yearly performed to verify that the key systems provides equivalent functionality and access to information through an equivalence test. The equivalence test should be performed as reperformance, desktop review and/or documentation verification to ensure verification of equivalence.
ITGC. 4	Inadequate access control and segregation of duties in key systems provides the incumbent retail organisation privileged access to information to the access seekers' operations.	**a)** The organisation has policies and procedures for access control and segregation of duties for the key systems in the retail and wholesale value chain, ensuring that beneficial information concerning the access seekers is not available to retail.
		b)The organisation regularly perform periodic review of user access to ensure segregation of duties to prevent that information relating to the access seekers in the key systems is accessible to retail.

VIII.Data/System risks and control objectives

Ref.	Risk	Control Objective
ITGC. 5	The organisation receives forecasts regarding the wholesale product volumes and uses this to gain a competitive advantage.	**a)** The organisation has designed and implemented a data asset register for retail and wholesale data, including a process which ensures that the data is kept separate.
		b) The organisation has an up-to-date overview of systems which contains business sensitive information related to wholesale customers.
ITGC. 6	Access seekers' lack of access to end user network information/data when there are faults in the network can result in lower customer satisfaction than for the incumbent's retail operation.	**a)** Measures are in place to ensure that access seekers have timely access to necessary end user network information/data in order to act as an intermediary, if necessary, in managing fault processes for its clients.
ITGC. 7	Inadequate access control and segregation of duties to relevant databases represents a risk of manipulation which would impact the integrity of the data the KPIs are calculated from. This is due to system owners and database owners having access privileges which can be leveraged to manipulate the data in the databases.	**a)** The organisation has implemented access control and segregation of duties to KPI relevant databases, i.e systems related to delivery management and fault repair.
		b) The organisation performs periodic reviews of the access to system databases regarded as relevant for the KPI process

VIII. Data/System risks and control objectives

Ref.	Risk	Control Objective
ITGC. 8	Lack of identificaiton and mitigation of risks associated with the key systems used in the retail and wholesale value chain could result in the inability to identify non-compliance with the non-discrimination obligation.	**a)** An identification and assessment of risks is performed for the key system used for wholesale customer follow-up for enquiries, product, orders and reporting of faults. [1*] Identified risks are evaluated and mitigation efforts are set out to minimise the risks to an acceptable risk level.
		b) An identification and assessment of risks is performed for the key system used for fault handling for customer reported and operational faults [8*] Identified risks are evaluated and mitigation efforts are set out to minimise the risks to an acceptable risk level.
		c) An identification and assessment of risks is performed for the key system used for calculating the possibility of technical delivery of broadband services to addresses [4*] Identified risks are evaluated and mitigation efforts are set out to minimise the risks to an acceptable risk level.
		d) An identification and assessment of risks is performed for the key system used for order and delivery registry for copper and fiber which forms the basis for invoicing [5*]. Identified risks are evaluated and mitigation efforts are set out to minimise the risks to an acceptable risk level.
		e) An identification and assessment of risks is performed for the key system used for overview of where the organisation can deliver fiber through availability checks based on the organisation's development [2*] Identified risks are evaluated and mitigation efforts are set out to minimise the risks to an acceptable risk level.

* The number represents a reference to an identified key system in the system architecture. See attachment for mapping of the respective key system.

VIII. Data/System risks and control objectives

Ref.	Risk	Control Objective
ITGC. 8 (cont.)	**(Continued from last page)** Lack of identificaiton and mitigation of risks associated with the key systems used in the retail and wholesale value chain could result in the inability to identify non-compliance with the non-discrimination obligation.	**f)** An identification and assessment of risks is performed for the key system used for machine-to-machine communication with external parties for business-to-business resale to register and validate orders for the wholesale broadband access portfolio. **[3*]** Identified risks are evaluated and mitigation efforts are set out to minimise the risks to an acceptable risk level.
		g) An identification and assessment of risks is performed for the key system used for testing and diagnosis of functionality for copper and fiber products in the value chain **[7*]** Identified risks are evaluated and mitigation efforts are set out to minimise the risks to an acceptable risk level.
		h) An identification and assessment of risks is performed for the key system used for booking resources for installation assignments for telephony, ADSL and communications products **[6*]** Identified risks are evaluated and mitigation efforts are set out to minimise the risks to an acceptable risk level.
ITGC. 9	Risk of a lack of access to historic data to confirm validity of historic KPI reporting.	**a)** The organisation has established a backup policy for KPI relevant systems enabling analysis of historic data.

* The number represents a reference to an identified key system in the system architecture. See attachment for mapping of the respective key system.

VIII.Data/System risks and control objectives

Ref.	Risk	Control Objective
ITGC.10	A lack of established change management processes for key systems and system interfaces represents a risk of incorrect and/or unauthorised changes adversely affecting the reliability of data.	**a)** A change management process is established covering all significant and non-significant changes to relevant systems and system interfaces, thus mitigating the inherent risk of adversely affecting the organisation's adherence to their non-discrimination obligations.
ITGC. 11	A lack of established change management processes for relevant databases represents a risk of incorrect and/or unauthorised changes adversely affecting the reliability of data.	**a)** The change management process includes the relevant database. This ensures that the databases holds reliable data, including historic data. The change management process includes separate test and production environments.
		b) The organisation's change management process is tested to ensure database changes are not implemented outside the change management process and that changes are done according to the process.

04 Attachments

Description of selected/potential key systems

Introduction to key systems

Described below are the systems the project has identified as key systems based on our understanding of the in-scope processes, dialogue with Telenor, Nkom and central access seekers, and the documentation provided by Telenor. Our definition of key systems is as follows:

- Systems/data sources used exclusively by access seekers
- Any system/data source with either a direct interface towards systems used exclusively by access seekers and/or a direct interface towards systems used by Telenor's retail operations for ordering, delivery, operation and maintenance of retail products associated with the regulated wholesale products.

Additionally, the system "Avtale" is considered a critical system due to its central functionality towards contractors.

Jara Netbusiness (1)
System used for access seekers' end user follow-up regarding enquiries, products, orders, and reporting of faults

VULA Web (2)
System used to provide overview of where the operators can deliver fiber through availability checks based on Telenor's development

Jara B2B (3)
System used for machine-to-machine communication with external parties for business-to-business resale to register and validate orders for the wholesale broadband access portfolio

KAPAKS (4)
System used for calculating possibility of technical delivery of broadband services to addresses

OMS (5)
System used for order and delivery registry for copper and fiber which forms the basis for invoicing

Avtale (6)
System used for booking resources for installation assignments for telephony, ADSL and communications products

Test and Diagnose (7)
System used for testing and diagnosis of functionality for copper and fiber products in the value chain

FHS (8)
System used for fault handling for customer reported and operational faults

Used by both Telenor and access seekers*

Used solely by access seekers

* System interfaces may differ between Telenor and access seekers

Act with integrity

Make a difference

Care

Work together

Reimagine the possible