Operator agnostic risk and control objectives over non-discriminatory controls in the Norwegian broadband market

December 2023

Version 2.0

Nasjonal kommunikasjons-myndighet

pwc

Disclaimer

This report has been prepared solely for Norwegian Communications Authority's use with the same type of purpose as set out in The Contract dated 2021-09-30. However, this operator agnostic version of the report may also be used in support of Nkom's enforcement of any non-discrimination obligations imposed on any broadband provider declared as a provider with Significant Market Power ("SMP") in forthcoming market analyses.

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, which was used in a public hearing Q1 2022. The engagement included detailing the risk and control objectives relevant for Telenor's non-discrimination obligations. This formed the basis for a third party attestation that Telenor is responsible for completing. The scope of the related control activities was determined by Telenor after Phase 2 completion. The time frame for the engagement was 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.

Executive summary

Background

In 2021, PwC was appointed by Nkom to prepare a risk and control matrix for the purpose of securing relevant controls within Telenor to demonstrate their compliance with the non-discrimination obligations imposed in the broadband wholesale marked decisions issued by Nkom. Nkom also decided that an external third party assessment of Telenor's non-discriminatory controls should be performed to demonstrate their compliance. Controls were to be based on the matrix of risks and control objectives outlined in the public report available on Nkom's web page. The process was yet to be completed by the time of preparation of this report.

Nkom considers this approach to secure effective compliance and enforcement could also be relevant to apply on any broadband providers with Significant Market Power (SMP) determined by an upcoming market analysis processes for the broadband markets in Norway. This operator agnostic risk and control matrix has been prepared for this purpose.

Approach

PwC's approach to prepare the 2022 Telenor risk control matrix included document review and process walkthroughs with Telenor, Nkom and central access seekers in the Norwegian broadband market, as well as a public consultation of a draft report. In the public consultation, comments were specifically invited on the potential application of a similar approach on any broadband providers identified as having SMP in the upcoming market review process.

Nkom and PwC both consider the risks and control objectives identified in the Telenor process likely to be relevant if Nkom decides to impose non-discrimination obligations on broadband providers identified as having SMP in the upcoming market review. It should be noted that:

- Organisational, process and system aspects may differ between Telenor and other broadband providers. Allowing the providers to propose controls within each control objective should allow for such factors to be taken into account. All controls are to be approved by Nkom.
- As the market review process is still at an early stage, Nkom may in their market decisions make adjustments of risks and/or control objectives contained in this report. Such adjustments may be of general nature, based on categories of providers or provider specific, if objectively justified. Nkom will consider consulting PwC for such assessments.

Summary

The objective of the attestation is to have an independent third party to verify how the provider adheres to their non-discrimination obligations for the fibre network. In this report – based on the similar report prepared for Telenor specifically - PwC have identified 41 unique risks, and 69 unique control objectives. These cover 7 central areas that are considered critical for a regulated broadband provider's ability to have a well-functioning internal control environment that ensures their non-discrimination obligations for the fibre network. Prior to being a part of any obligations imposed in the upcoming market review process, also this report will be a part of a public hearing.

The 7 central areas with identified risks and related control objective include:

- Entity Level
- Fault repair
- IT General Controls
- Coverage information prior to order
- Monitoring of KPI
- Order and delivery
- Test and Diagnosis

01 Background and scope

Background and scope

Background

At the time of preparation of this report, it's not an unlikely outcome of the upcoming market review process that one or more broadband providers are identified as provider(s) with Significant Market Power ("SMP"). The experiences from enforcement of non-discrimination obligations under previous market review processes, as well as the potential identification of several provides with SMP in the upcoming market review, has led Nkom to consider a more internal control based approach to compliance and enforcement. An external third party assessment of the controls identified is, in Nkom's assessment, an appropriate measure to ascertain whether the non-discrimination obligations are complied with. Nkom has an ambition of increasing trust, openness and transparency with regards to the non-discriminatory practices and internal controls of any broadband provider on which Nkom has imposed non-discrimination obligations. To achieve this, Nkom will consider to impose on any such provider(s) to demonstrate their compliance through a third party assessment of their non-discriminatory controls.

Scope of the engagement

PwC was engaged by Nkom to develop a risk and control matrix to be applied by Telenor in 2022. Based on this delivery, PwC was engaged by Nkom to also prepare this operator agnostic report, set to identify and detail applicable risks and control objectives that are likely to be relevant for actual or potential anti-competitive behaviour by any broadband provider in the Norwegian broadband market identified by Nkom as having SMP. In addition to being the platform for internal controls, the matrix could also form the basis of a third party attestation with the objective of verifying whether the provider adheres to their non-discrimination obligations.

All risks and control objectives listed in the control matrix may not be applicable to all providers with SMP. Risks that are not applicable may be scoped out, after approval from Nkom. The key systems that the risks and control objectives are applicable for should be identified by the provider with SMP, and approved by Nkom.

Expectations and next steps (1/2)

Expectations for broadband providers with Significant Market Power

Nkom has an expectation that providers with SMP will map their control activities to the risks and control objectives documented as part of this engagement. These control activities should subsequently be tested by an independent third party and be presented in a recognised third party attestation standard, such as ISAE 3000*. The 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 providers with SMP perform an equivalence test to verify that the key systems provide equivalent functionality and access to information. The assessment should be executed by an independent and objective party independent from the provider with SMP. 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 attestation, or equivalent.

1 Final risk and control matrix approved by Nkom

Key tasks:
- Input/feedback from stakeholders following the public hearing was considered
- Nkom approval of finalized version of the risk and control matrix

2 Identification of key systems applicable for the process

Key tasks
- SMP providers to identify key systems applicable relevant for their non-discrimination obligation
- Nkom to approve key systems
- If the SMP provider believes certain risks and/or control objectives are not applicable to their operations, Nkom may consider approving certain scope changes

3 SMP provider to confirm control activities to address risk and control matrix

Key tasks:
- SMP provider to develop and map control activities to identified risks and control objectives in the risk and control matrix
- SMP provider 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 the SMP provider's controls

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

5 SMP provider to obtain an ISAE 3000 third party attestation

Key tasks:
- SMP provider to engage a third party to carry out the third party attestation
- SMP provider to present the attestation report to Nkom

***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. The provider with SMP 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 the SMP provider'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 the SMP provider'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

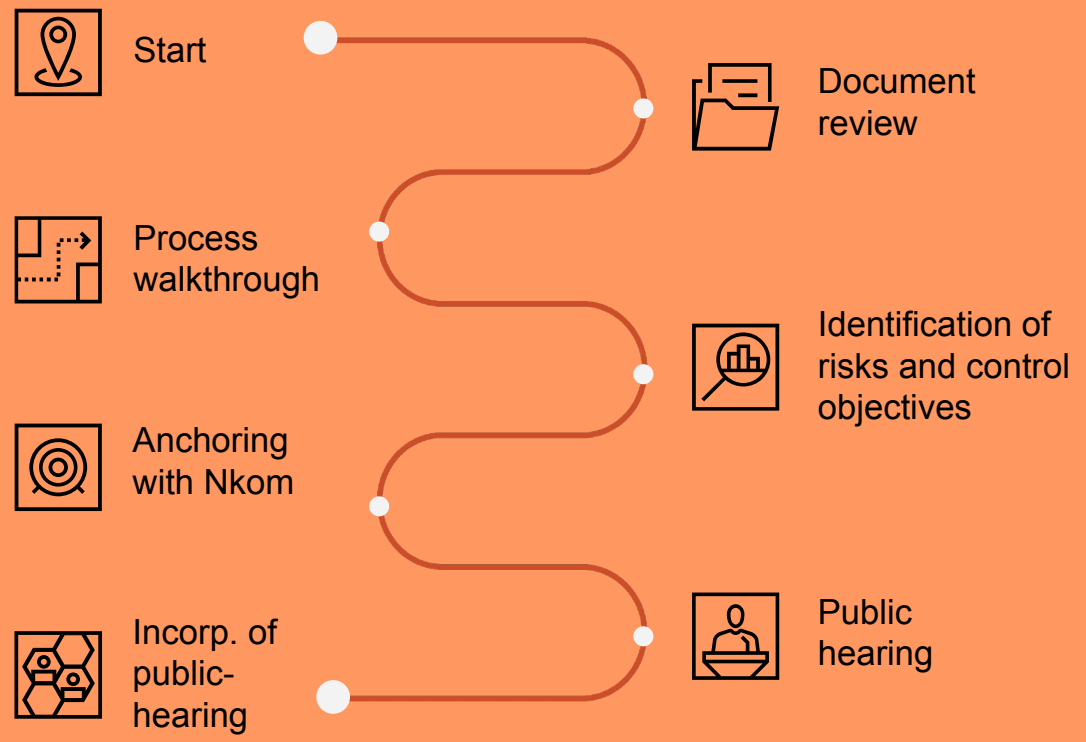
Methodology

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

Nkom and PwC consider the output based on this methodology to be relevant for any other provider identified as having SMP, notably because of the freedom of the provider to suggest controls based on own circumstances within the risks and control objectives defined in the matrix. Nkom's experience working with other NRAs in the EEA area also indicates that those risks and control objectives defined seem to be in line with the regulatory regime in other markets.

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 that can help an organisation identify, implement and/or mitigate risks. The framework is a repository of risks that may pose a threat to an organisation's non-discrimination obligation, and control objectives to mitigate those risks.

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

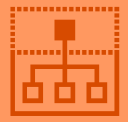
- Entity Level
- Fault repair
- Test and Diagnosis
- Coverage information prior to order
- Monitoring of KPI
- IT General Controls (ITGC)
- Order and delivery

The intended use of the risk and control matrix

The risk and control matrix will provide SMP providers 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[1]. This will complement their compliance efforts with regards to their non-discrimination obligations and provide assurance over the completeness of their efforts. The SMP providers' documented control activities, along with the risks and control objectives, will form 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 the SMP providers with the opportunity to objectively demonstrate their adherence to their non-discrimination obligations.

[1] Some risks and/or control objectives may be out-of-scope for certain operators. Any such exclusions should be discussed with and approved by Nkom.

Risk and control matrix



Rationale for the breakdown
The risk and control matrix is segmented into seven, logical groups. The groups include areas and processes identified as critical for SMP providers' 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 the provider with SMP'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 the provider with SMP.

Order and delivery
Risks and controls relate to the SMP provider'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 the provider with SMP 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.

Operations (excl. fault repair)
Risks and controls refer to non-discrimination related to the SMP provider'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 SMP provider's systems and data.

Description of selected/potential key systems

Introduction to key systems

The provider with SMP is responsible for identifying key systems for their non-discrimination obligations, based on their understanding of relevant processes, interface dependencies for the systems used by retail and wholesale value chain. The key systems are to be reviewed and approved by Nkom. This is likely to at least include:

- 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 the SMP provider's retail operations for ordering, delivery, operation and maintenance of retail products associated with the regulated wholesale products.
- Systems with central functionality towards contractors

I. Entity level controls risks and control objectives

Ref.	Risk	Control Objective
ELC.1	**Tone at the top** The tone at the top does not include clear directions for employees to ensure their non-discrimination obligations.	**a)** There have been established governing documents such as organisational strategy, policies and procedures that explicitly communicate employees' responsibilities to prevent non-compliance with the obligations in laws, regulations and NRA decisions related to electronic communications. **b)** Management has ensured the establishment of control mechanisms to detect and address any misconduct that may arise related to their non-discrimination obligations. Such mechanisms should include: • Clearly defined and communicated employees' duty to report incidents and deviations from their non-discrimination obligation and established control framework. • Whistleblowing hotlines for staff to report misconduct and procedures to handle any reported deviations. Any possible deviations are quickly identified, assessed and, if necessary, reported. The need for compensating controls to prevent similar deviations/incidents from occurring is assessed and implemented in a timely manner as needed. **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 non-discrimination obligation. **f)** Management has established and implemented effective mechanisms to ensure that policies and procedures are known and complied with in the organisation.

I. Entity level controls risks and control objectives

Ref.	Risk	Control Objective
ELC.2	**Risk assessment and management** Management fails 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 analyses related to risk of non-compliance with the non-discrimination obligations, and in addition also performs such an analysis on their own initiative.
		b) Management regularly assesses the need for risk reducing measures based on completed risk assessments. Measures to eliminate or reduce the risk of actual and potential non-compliance are performed timely and documented accordingly.
ELC.3	**High barriers to entry** 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 assesses 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, office location, governance arrangements and bonus schemes.
ELC.4	**Information and communication** Management fails to communicate information to the employees 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. The Code of Conduct is communicated and understood by all relevant employees.
		b) The organisation regularly assesses 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.5	**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 supports access seekers attempting to enter the Norwegian broadband market, ensuring that they have the necessary information to enter a partnership with them. Information includes details such as planned technology changes and infrastructure roll-out etc.
ELC.6	**Monitoring activities** Management fail to develop and perform evaluations to ascertain whether the organisation adheres 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 independent representation, company/group external 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.7	**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 ensure 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 about the emergency. **b)** The organisation conducts analysis after emergencies to assess compliance and identify improvement areas/guidelines for similar events in the future.

II. Coverage information prior to order risks and control objectives

Ref.	Risk	Control Objective
PCIPTO.1	**Information sharing** The process for sharing information regarding coverage prior to order does not have clear directions for employees to be sufficiently informed about their responsibilities for non-discrimination.	**a)** Clearly defined policies and procedures are established and implemented for manual operations related to coverage information prior to orders. The internal policies and procedures provide directions related to the employee's non-discrimination responsibilities. All employees are aware of their non-discrimination duties.
PCIPTO.2	**Information sharing** 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 and interface functionality through coverage search and web based direct retail customer requests. **b)** The organisation periodically performs 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	**Information sharing** Access seekers do not receive coverage information in accordance with the timeliness obligation.	**a)** The organisation regularly performs 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 delay unless otherwise regulated in the SMP decision.

III. Order and delivery risks and control objectives

Ref.	Risk	Control Objective
POAD.1	**Order and delivery process** The process for order and delivery 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 and implemented for manual operations related to order and delivery. The internal policies and procedures provide directions related to the employees' non-discrimination responsibilities. All employees are aware of their non-discrimination duties.
POAD.2	**Subcontractors** Subcontractors favour retail deliveries over access seekers deliveries. *Applicable only where the subcontractor has access to information on whether the order/delivery is associated with a retail or an access seeker's customer.*	**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	**Subcontractors** Communication with subcontractors are not equally accessible to/from retail business and wholesale customers during the delivery process	**a)** Measures are in place to ensure communication with subcontractors are equally accessible and ensures end users have relevant information about the delivery process.

IV. Operations risks and control objectives

Ref.	Risk	Control Objective
PO.1	**Test and diagnosis** 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 and implemented for manual operations related to test and diagnosis. The internal policies and procedures provide directions on the employees responsibilities related to non-discrimination and ensure all employees are aware of their non-discrimination duties.
PO.2	**Systems for test and diagnosis** 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 have the same level of quality for retail as for access seekers.
PO.3	**Systems for test and diagnosis** Access seekers do not have the same 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 prerequisites as retail do. Measures to secure fair prerequisites may include effective and equally accessible training material and support in using the tool
PO.4	**Information and communication** 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 and implemented outlining how incidents are handled and communicated externally to access seekers.

V. Fault repair risks and control objectives

Ref.	Risk	Control Objective
PFR.1	**Discriminating fault repair** The organisation prioritises the fault repair for their own retail customers over those of access seekers.	**a)** Clearly defined policies and procedures are established and implemented for manual operations related to fault repair. The internal policies and procedures provide directions on the employees responsibilities related to non-discrimination and ensure all employees are aware of their non-discrimination duties.
PFR.2	**Subcontractors** Subcontractors favour retail fault repairs over access seekers' fault repairs. *Applicable only where the subcontractor has access to information on whether the fault repair is associated with a retail or an access seeker's customer*	**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 has controls in place to identify and handle incidents where subcontractors could favour fault repairs for retail over the access seekers.
PFR.3	**Customer poaching** The organisation actively contacts the access seekers' customers when there are faults in their broadband services to incentivize them to become customers of their own organisation instead.	**a)** An assessment has been made to identify situations where the poaching of customers would be in conflict with their non-discrimination obligations. Internal procedures are established and implemented for the communication with customers during such instances. This ensures that access seekers' customers are not incentivised to leave the access seekers in such instances.
PFR.4	**Subcontractors** 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	**KPI monitoring process** Monitoring and follow up of KPI reporting do not have clear directions for the employees to be sufficiently informed about their responsibilities related to non-discrimination.	**a)** The process to prepare, monitor and follow up KPI reports is supported by clearly defined policies and procedures. The internal policies and procedures provide directions related to their non-discrimination and access obligations.
PMOKS.2	**Accurate and complete KPIs** The organisation's reported KPIs are not complete and accurate, including inaccurate definitions and carve-out of populations, making reporting of absolute performance levels and comparisons across retail and wholesale unreliable.	**a)** There have been established and implemented policies and procedures for the design of KPIs, including accurate definitions with product segmentation and any filtering of populations. This enables follow-up of absolute performance levels and – where imposed - comparisons of performance between retail and wholesale. **b)** The organisation ensures that the preparation of KPI reports is aligned with the framework established through 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 to ensure the integrity of the KPI reports. **d)** There has been established and implemented a policy and procedure(s) for the change management of the KPI design, methodology and reporting. Changes to the KPI design are done in accordance with policy and procedure(s). **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)** The organisation regularly evaluates the data generation process to validate the integrity of the process. This includes 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 annual, independent review of the KPI process to verify the integrity of the process and relevance of established KPIs. Any deviations are identified and addressed as needed. *Nkom may on request grant exemption from the review taking place annually.*

VI. Monitoring of KPI/SLA risks and control objectives

Ref.	Risk	Control Objective
PMOKS.3	**KPI deviations** 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 the statistical significance of the deviation, which will segment out following up of falsely identified deviations.
PMOKS.4	**Information and communication** The KPIs, including the methodology, KPI design, and specification, are not available for relevant stakeholders in a timely manner.	**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 publishes the KPI reports on their website within 15 working days of the end of the reporting period.
PMOKS.5	**Manual data processing faults** Manual data processing faults occur prior to KPI publishing, impacting the accuracy and integrity of the KPIs.	**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	**KPIs not aligned with quality targets** 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	**Information and communication** Access seekers do not have accurate and complete information about the delivery and fault repair of their respective lines.	**a)** The organisation has policies and processes in place that ensures access seekers have access to the underlying data related to their own products on request and/or through monthly service reports.

VIII.Data/System risks and control objectives

Ref.	Risk	Control Objective
ITGC.1	**System and dataflows** Management does not maintain a list of systems and dataflows able to support their compliance obligations.	**a)** Management annually reviews and approves the scoping of key systems for broadband services, relevant for their non-discrimination obligation.
		b) An up to date list of data and systems, including data flow, is established. Management reviews the list periodically and after any significant changes, to maintain necessary oversight of the non-discrimination aspects of system architecture and key systems.
ITGC.2	**Undefined system architecture** 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 creates insufficient transparency for internal and external oversight of compliance with the non-discrimination obligations.	**a)** Management regularly reviews and approves the individual system descriptions, system architecture and dependencies per relevant key system in scope.
ITGC.3	**Opportunity for automation** Access seekers do not have the same opportunity to automate their processes.	**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.

VIII. Data/System risks and control objectives

Ref.	Risk	Control Objective
ITGC.4	**Unequal system functionality and opportunity** 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)** The organization ensures on an annual basis, through independent and objective assessments, that the key systems for wholesale and retail provide non-discriminatory functionality, and non-discriminatory access to information. *Nkom may on request grant exemption from the assessment taking place annually.* The control objective includes but is not limited to the following elements: • ensuring that the non-discriminatory information and functionality is available for both retail and access seekers regarding information prior to order, during the order and delivery process, test and diagnosis process, and the fault repair process for their respective customers • ensuring transparency with regard to what tests are performed independently by third parties, and what tests are performed by internal resources with a subsequent documentation review by the auditor. Unless and until otherwise agreed upon with The Norwegian Communications Authority (Nkom), the requirement for the assessment to be performed by an independent third party remains. • ensuring that the documentation is at a sufficient level of detail, which enables an independent and external party such as Nkom to assess that the functionality and information supports the non-discriminatory objective. This also includes relevant system interfaces.
ITGC.5	**Access controls to key systems** 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 implemented policies and procedures for access control and segregation of duties for the key systems in the retail and wholesale value chain, ensuring that confidential information concerning the access seekers is not available to retail. **b)**The organisation regularly reviews user access to ensure segregation of duties and the principle of least privilege[2] to prevent that information relating to the access seekers in the key systems is accessible to retail.

[2] Defined by ISACA as “Controls used to allow the least privilege access needed to complete a task”.

VIII.Data/System risks and control objectives

Ref.	Risk	Control Objective
ITGC.6	**Segregation of data** The organisation receives forecasts about the wholesale product volumes and uses this to gain a competitive advantage.	**a)** The organisation has designed and implemented appropriate processes and controls to ensure that the data related to retail and wholesale operations are kept separate.
		b) The organisation has an up-to-date overview of systems that contains business sensitive information related to wholesale customers.
ITGC.7	**Information and communication** 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.8	**Access control to databases** 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
ITGC.9	**System risks** Lack of identification 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 all key systems. Identified risks are evaluated and mitigation efforts are implemented to minimise the risks to an acceptable level.

VIII.Data/System risks and control objectives

Ref.	Risk	Control Objective
ITGC.10	**Backup and recovery** Lack of access to historic data prevents verification of historic KPI reporting.	**a)** The organisation has established and implemented a backup and recovery policy for KPI relevant systems, ensuring the availability of historic data relevant for KPI reporting.
ITGC.11	**Change management** 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 implemented for all 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.12	**Change management** 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 is implemented for relevant databases. 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.

Act with integrity

Make a difference

Care

Work together

Reimagine the possible