RISK MANAGEMENT GUIDANCE

Introduction

Tele2 recognizes risks which are associated with achieving the company objectives. Managing these risks forms an essential part of the business. The aim of risk management within this company is to provide reasonable assurance that we understand the risks associated with achieving our business objectives and that we are responding appropriately to these risks at all levels within our organization.

This is achieved by ensuring that at all times:

1. Risks are properly identified, assessed, managed and reported;
2. Risk ownership is taken and communicated;
3. Resources are effectively and efficiently allocated to manage risks;
4. Risks that could significantly affect our employees, the company, our suppliers / vendors or our customers are suitably managed;
5. The company is compliant with regulatory and legal requirements.

Risk management should not be treated as a separate activity but as an integrated part of any activity, process or function. Anyone with responsibility over a certain market, function, process, project etc. inherently also needs to assess the risk of not being able to deliver what is expected of him or her and to take measures to improve the chances of success. This implies that every employee has a responsibility for risk management over the area of his or her responsibility.

This document aims to provide guidance to staff and management for how risk management and internal controls could be developed and maintained throughout the whole organization.

Risk Management

There are several ways to look at and classify risk. Tele2 categorizes its risk into four main categories - Strategic, Operational, Financial and Compliance. The following picture illustrate how this concept applies to Tele2:

Another way of classifying risk is by distinguishing between internal and external risks. Whereas internal risks depends a lot on the specific circumstances of the business and could be more or less infinite in numbers external risks (and opportunities) are generally presented by changes in one of the following illustrations:

- Competitive activity
- New technology
- Changes to legal or regulatory requirements
- Major fluctuations in financial markets or macro economy
- Major geopolitical events
- New paradigms in public opinion
- Environmental changes
- Hazards, pandemics and disasters

Even if no change, these areas still presents limitations and constraints to which the business need to relate, especially regarding legal and regulatory requirements for which there might be a risk of non-compliance to existing requirements.

Regardless of classification or what type of risk, risk management ideally includes the following key steps:

1. Risk Identification and assignment of Group Leadership Team owner
2. Risk assessment
    a. Identification of risk areas
    b. Identification of events/scenarios within each risk area
    c. Assessment of impact and likelihood
    d. Risk vs. existing controls - Gap analysis (residual risk identification)
3. Risk Prioritization
4. Risk Response
5. Risk monitoring and reviews

Risk Management stages in detail

1. Risk Identification and assignment of Group Leadership Team owner

   Risk Management begins with Risk Identification, which involves identifying any possible threat or vulnerability which may adversely affect Tele2's Purpose.

   Risk identification is the mechanism of identifying exposure to uncertainty across the organization. This involves assessment of the external and internal environment in which the firm operates and recognizing risks that can impact the achievement of the company's strategic and operational objectives. Risk identification is an ongoing activity.

   Risks identified can be segregated into two levels:

   a. Enterprise-wide Risks – These are strategic risks that have a mid to long term impact on Tele2, including operational risks that have a strategic impact on the organization.
   b. Process level Risks – These are operational risks that have a current to short term impact on the operational activities and tasks. These risks are faced by the operational teams on a periodic basis due to the ongoing operations of the company. As a part of the company's internal assurance program, the Internal Audit department must test these checks and controls to gauge the operational effectiveness of the processes and business functions.

   Risk Drivers

   As a part of the risk identification process, it is also important to understand which of the business drivers are impacted by the materialization of a risk or any of its root causes. These business drivers represent the signals of change to be used for identifying the underlying risks. This list is drawn from internal and external environment factors. The Group Leadership Team and Process Owners use these drivers on a quarterly basis to identify and report on events/ incidents that have occurred and would lead to a new risk/ event.

   Assignment of Risk owner

   A Group Leadership Team member is assigned the identified risk to manage it further down the organization.

   Risk Register

   A risk register acts as a central repository for risks. The purpose of the risk register is to identify and record risks and related information in a structured manner. The ownership of individual risks will lie with Group Leadership Team owners at the Group or country.

   The Head of Internal Audit assists the Group Leadership Team in risk identification, creating and updating risk registers (detailed later in the guidance document). However, it is the responsibility of each entity and business line to identify risks relevant to their organizational setup and objectives which rolls up to the Leadership Team owners at the Group or country.

2. Risk scenario identification and risk assessment

   Risk scenario identification and risk assessment refers to the process followed for understanding the nature and level of risk. It involves the determination of quantitative or qualitative value of risk. It also requires the calculation of the potential loss or impact, and the likelihood that the loss will occur. It is performed for each risk identified. The onus of risk assessment lies with the risk identifier/ owner.

   Risk assessment provides the inputs requisite for evaluating the risk response. Based on the results of the assessment, an appropriate action to be taken for risk response is decided.

   Risk assessment is based on the following parameters:

   - Time to manifest – How quickly is the risk likely to manifest
   - Calculate likelihood of risk events
   - Calculate potential impact of the identified risk scenarios

   The assessment of each risk would be done in two stages:

   - Considering the impact and the likelihood of the events without taking any mitigation actions
   - Considering the impact and the likelihood of the events if actions for mitigation are taken

The four risk categories described above can be used to structure the assessment by setting and linking objectives to either strategy, operations, financial/reporting or compliance and assessing each area at a time.

It is recommended to assess the risks in two steps; first identifying high level critical **risk areas** (e.g. "Strategy execution" or "Customer Experience") and; secondly identifying more specific **events/scenarios** that could potentially trigger an adverse impact on the objectives. Generally the high level risk areas do not change much over time whereas the risk events/scenarios do, which means that the latter has to be monitored more closely. As an example, "Spectrum" has been identified as one of the Tele2 group's most important risk areas[1]. On this level the risk is not expected to change any time soon. However, within this area events, which in this case usually are defined as the risk of losing a particular upcoming license auction, constantly has to be updated based on what the regulators decides in our different markets.

In order to get a more focused discussion and to relate the risks to the strategy Tele2 defines a risk appetite meaning the level of risk that the entity is prepared to accept in pursuit of its objectives.

Assessing the **impact** of the risks is preferably done by assigning a monetary value corresponding to the revenues that could be lost or costs that could be incurred if a risk scenario materializes. For **likelihood** the preferred way is to assign a percentage. Alternatively, relative terms such as High/Medium/Low are used for both impact and probability.

The initial risk assessment is done without considering already existing control mechanisms. This is what is referred to as identifying the **inherent risk**. To this management then needs to consider existing controls (i.e. existing policies, procedures, system/process controls etc.) and evaluate whether these are sufficiently mitigating the risk (considering the risk appetite if such has been defined). If not, then management needs to define additional controls and actions to mitigate the "**residual risk**".

There are various possible responses to a risk. However, the most common is to try and "reduce" the risk by implementing additional controls. Other possible responses include "accepting" the risk (without additional controls), "transferring" the risk, which could be done through insurance, or totally "avoiding" the risk, which however usually means stop pursuing the corresponding opportunity.

In order to visually depict the risk assessment based on 'residual risk', a "risk matrix" (graphical representation of impact and likelihood) is used based on the risk analysis (i.e. Likelihood * Impact) wherein each risk will be plotted based on its relative likelihood and impact.

3. Risk Prioritization

Risk prioritization is the process for prioritizing risks having a residual risk, based on whether the risk and its magnitude is acceptable or tolerable within Tele2's risk appetite. Risk prioritization is done by each risk owner and collectively vetted by the Leadership Team.

4. Risk Response and identification of actions

Risk response is treatment of the risk identified post assessment and prioritization. This requires the mitigation owner to select one or more options for managing and treating risks, and implementing the agreed mitigation/ action plans. This phase of the ERM process is intended to:

- Understanding and ensuring existing controls/ mitigation mechanisms are in place for managing and treating risks
- Generate a new risk response plan if the existing controls are ineffective and/ or need to be strengthened to respond to the identified risk
- Continuously assess the effectiveness of such response plans

A risk response may fall into any of the 4 following categories namely:

- Avoid - Exiting the activity giving rise to the risk

- Reduce - Action is taken to reduce risk likelihood or impact, or both
- Share - Reducing risk likelihood / impact by transferring /sharing a portion of the risk
- Accept - No action is taken to affect risk likelihood or impact

Risk response can be a choice from the above or a combination of multiple options.

5. Risk monitoring and reviews

Risk monitoring is conducted on a periodic basis, for the identified risks, in order to track the status of response plans and to consequently update changes to risk profiles.

Risk reviews involves re-examination of the risk register, risk assessment and risk response including the risk profiles. The risk review is conducted to monitor the effectiveness of the ERM framework. Risk reviews entail updates to the risk register with updated risk assessment, new/emerging risks, and the related responses and profiling. The risk reviews are carried out at least on a quarterly basis and updated in the risk report.

Internal controls

Internal controls support Tele2's risk management and drives our risk culture. Tele2's framework for internal controls is based in part on the COSO model which defines internal controls as:

- *"a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance"*

Further to above, internal controls is defined as consisting of the following five components:

1. **Control Environment** - Sets the tone for the organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control
2. **Risk Assessment** - The identification and analysis of relevant risks to the achievement of objectives, forming a basis for how the risks should be managed
3. **Information & Communication** – Systems, processes and documentation that support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities
4. **Control Activities** - The procedures that help ensure management directives are carried out
5. **Monitoring** - Processes used to assess the quality of internal control performance over time

Below is an illustration of how these components apply to Tele2, with examples of what is included under each component.

Tele2's Internal Control philosophy

The Tele2 Group and its geographical footprint has undergone significant change during the past two years. After the merger of its Swedish operations with Com Hem, the Swedish market is approximately 80% of the total Tele2 Group. Due to this, the governance responsibilities towards maintaining Internal Control over Financial reporting has also been restructured.

The responsibility for maintaining an effective control environment and ongoing work on internal controls has been assigned to the President and Group CEO and documented in the "Instructions to the Managing Director of Tele2 AB". The President and Group CEO has, in turn, allocated responsibility for maintaining internal controls to the Tele2 Leadership team and his direct reports.

The line managers are inherently responsible for the risk identification and risk mitigation related to their respective market or corporate area for financial reporting and other operational processes. On top of this, Internal Audit performs a risk assessment for each market and function (including financial reporting) which forms the basis for the annual internal audit plan. This risk assessment considers the fact that there is risk both from how we operate and from where we operate.

Other inputs to this risk assessment and the internal audit plan include results of prior audits, known incidents and reporting issues, external risk benchmarks and external assessments of countries' general corruption levels, etc. The internal audit plan is reviewed and approved by the Board through the Audit Committee.

The overall control environment in Tele2 is much influenced by our common values which are reflected in all parts of our business, from trainings for new employees to developing corporate strategy.

There are also control activities in place to ensure that the values are, not only known by employees and managers, but also that we act in accordance with them, i.e. that we "walk the talk". All employees are evaluated against these common values and managers are required to conduct training on "The Tele2 Way" in order to discuss and gain greater insight into the company's values and practices.

Another key aspect of the overall control environment is the Executive Management's enforcement of the Tele2 Code of Conduct and, as part of this, the four-eyes principle, which means that important decisions and contracts signed on behalf of Tele2 should always be made by at least two persons. The Code of Conduct is signed by all employees upon joining Tele2 and then reconfirmed annually. All employees are accountable for compliance with the code of conduct. When entering into a contractual arrangement with Tele2, suppliers and other business partners also need to give their assurance regarding compliance with Tele2's standards by signing Tele2's Business Partner Code of Conduct.

Also, our whistleblower process ensures that anyone working for or with Tele2 can report any wrongdoing. It also provides protection to any individual making a report of potential misconduct. We have implemented low-threshold possibilities for reporting any wrongdoing related to Tele2. Reporting can be done either anonymously, confidentially or openly and through different methods. Members of the Group Leadership Team and the Board (including the Audit Committee) are informed ad-hoc of ongoing or concluded investigations.

Internal Controls maturity assessment

The table and questions below, which is based on the COSO model described above, is provided as a guide for management for how to benchmark and improve internal controls within the organization. The table is generic and could be used for any type of entity, from corporate level down to a department within a particular group function or country.

Component	Internal Controls Best Practices
Control environment	• Stakeholder expectations are clear and articulated/aligned with the objectives and responsibilities of the entity (department/country/market area/function/Tele2) • Management of the entity acknowledges their own responsibility for ensuring efficient and well controlled procedures throughout the whole organization • The entity has a clear mandate and clear escalation procedures • Sub-departments' and Individuals' responsibilities are clearly defined and understood
Risk assessment	• Risks relevant to the geographical and/or functional area of responsibility and the entities objectives are proactively identified and evaluated, including: o Risks impacting services, costs, revenues etc. (operational risks) o Risks impacting the financial representation/reporting of the operations (financial/management reporting risks) o Risk of non-compliance to laws and regulations or to internal policies and procedures (compliance risks) o Risks with potential impact on strategic or financial objectives (strategic risks)
Information & Communication	• The boundaries within which the business should operate have been defined and articulated (e.g. in a policy) based on, and in order to mitigate, the key risks • Proper communication and training is provided for areas of importance
Control activities	• Process controls at country and/or central level are implemented to ensure key risks are mitigated (risks and issues are either prevented or detected/corrected) • Exceptions to policies are appropriately approved
Monitoring & follow-up	• Compliance to policies and the performance of process controls is periodically evaluated by the entity and used as input to the risk assessment and for clarifying and making changes to policies and procedures • Significant risks, control gaps and policy exceptions are continuously monitored and escalated to appropriate level • Internal and external audit issues are adequately addressed and escalated

In implementing or improving internal controls within an entity management considers the best practices table above in chronological order, hence, starting with ensuring a sound **control environment**, including that stakeholder expectations are known and that the objectives of, and responsibilities within, the entity (e.g. department) are clearly defined and agreed.

The **risk assessment** is based on stakeholder expectations and objectives of the entity and with consideration of potential external and internal constraints and threats as explained in the Risk Management section above.

Information and communication is in the form of policy or other instructions. If properly based on risks, and if monitored and followed up, policies could also be considered a control activity in that it helps limiting or mitigating the risks. For practical reasons however not all risks can be controlled via policies which is why automating controls by use of IT systems (e.g. a system based invoice approval flow) or integrating controls in standard processes is also needed.

Control activities include any activity that help either *preventing* something (the risk) from happening or *detecting* that something has happened. Hence, controls can be either preventive or detective as illustrated in the examples below. Additionally controls can be more or less effective depending on the nature of the control. For example, a written work instruction for system managers telling them all new users to a system needs to be approved by the business system owner is most likely less effective than having an automated authorization system which does not allow new users unless approved by the system manager.

Different controls may also target different things, like ensuring *restricted access*, ensuring that transactions are *complete* and/or *accurate* or that the transactions are *valid* (i.e. that there is a proper business need for it). Generally several controls are needed to fully mitigate one risk.

Risk event/scenario	Control activity (examples, non-exhaustive)	Preventive or detective
Unauthorized/uncontrolled increase of employee costs	Grandfather approval and HR review before entering new salaries in system	Preventive
Incorrect financial reporting of sales	Reconciliation of Financial Statement to billing system/-s	Detective
Incorrect or fraudulent purchases	System invoice approval flow ensuring approval by cost centre responsible and manager (4eyes princ.)	Preventive
Incorrect or fraudulent payments	Restricted access to payment system	Preventive
Incorrect or fraudulent payments	Supervisor's review of payments made	Detective
Loss of data or production capacity due to system crash	Back-up and restoration procedures/instructions	Preventive
System failure due to incorrect maintenance	Separated development and production environment	Preventive
Failure to comply with data privacy requirements	Periodic compliance risk assessment by Data Privacy Officer	Both

In a fully developed and mature organization management do not only identify risk and communicate requirements and controls but also **monitor and follow up** how those requirements are managed and how controls are performed in order to be able to reassess the risks over time.

Governance

The ERM Governance identifies the key internal stakeholders responsible for creating, implementing and sustaining ERM. At Tele2 this structure is the same as the Governance structure adopted by Tele2 and as described in detail in the Corporate Governance section of the Annual Report.

Board of Directors and Audit Committee

With respect to Risk Governance, the Board of Directors and Audit Committee have the following responsibilities:

- Determine the strategic direction of the organization
- Establishing expectations with respect to Enterprise Risk Management
- Reviewing and approving risk management related policies, procedures and parameters
- Allocating adequate resources for treating critical risks and/ or risk events at the organization level
- Owning risks of strategic importance impacting Tele2 at an organizational level, and establishing a risk environment that is consistent with accepted group practices and fulfils the expectations of the shareholders
- Reviewing the critical aspects of the Tele2s overall risk profile through the periodic review of high-level reports that address material risks and strategic implications
- Endorsing the Enterprise Risk Management organization structure and authorizing roles and responsibilities for key stakeholders

Executive Management

Perform tasks outlined the section 'Risk Management stages in detail'

Enterprise Risk Management Support

The responsibility of supporting the ERM process lies with the Head of Internal Audit. The independence of the Internal Audit Function and the responsibility of Enterprise Risk Management is ensured through the best practice reporting line to the Audit Committee of Tele2 AB. He has a dotted line administrative reporting to the CFO of Tele2 AB. The following are his responsibilities:

- Design and review the processes for risk management
- Establish and communicate the organization ERM vision
- Provide support on risk management to the Executive Management:
    i. Regular discussions with country CEO and CFO, Group heads and Group Leadership Team on various risk topics (existing and emerging).
    ii. Participation in monthly country and Group finance meetings organized by the Group CFO to discuss top topics and risks. Participation in various committees where top events, issues, risks and their treatment is discussed.
    iii. Analyze and update the Risk register - Initiate dialogue on various topics with the responsible Group LT member to determine if an emerging risk has potential to be elevated as a strategic risk or a new risk category needs to be created.
    iv. Document and follow up with Executive Management on existing strategic risks
    v. Conduct or facilitate training and risk workshops with various levels of the company
    vi. Encouraging relevant stakeholders on the approach for robust impact and probability assessments through financial analysis. More non-financial topics sometimes require independent expert assessments.
    vii. Evaluate the quality of risk management through adequate internal control and risk mitigation activities through annual internal audit plans formally approved by the Audit Committee and reporting results of the audits directly to the Board through the Audit Committee.
- Maintain regular communication with the Board through discussions and updates on risk management through the Chairman of the Audit Committee.
- Provide continuous training in the form of quarterly risk updates to the Audit Committee and an annual update to the Board.