# Financial Stability Board "Principles for an Effective Risk Appetite Framework 2013": Defined FSB Role Responsibilities[i] and Objective-Centric Risk & Certainty Management ("ORCM") Enablers

**NOTE: "RAF" is the FSB short form for Risk Appetite Framework**

## 4.1 The board of directors should:

a) approve the financial institution's RAF, developed in collaboration with the CEO, CRO and CFO, and ensure it remains consistent with the institution's short- and long-term strategy, business and capital plans, risk capacity as well as compensation programs;

**ORCM Enablers**: ORCM provides a comprehensive response to build an effective RAF that links to top value creation and value preservation objectives with specific attention being paid to regulatory responsibilities. Objectives linked to risk capacity/solvency and other areas of regulatory focus can be explicitly assigned to OWNER/SPONSORS, risk/certainty assessed, and the status reported on to CEOs and boards on a regular basis.

b) hold the CEO and other senior management accountable for the integrity of the RAF, including the timely identification, management and escalation of breaches in risk limits and of material risk exposures;

**ORCM Enablers**: In an ORCM framework the CEO and C-Suite play key and highly visible roles overseeing the organization's risk governance framework. Specific responsibilities are defined in the entity ORCM policy or equivalent. The CEO and other C-Suite executives receive regular reports on effectiveness of the framework from risk management (2nd line) and Internal Audit (3rd line), and are expected to regularly report to the board on integrity of RAF and all incidents where current OBJECTIVE CERTAINTY for specific objectives is rated as unacceptable/outside of risk appetite/tolerance. The ORCM Six Level Quality Assurance framework also allows CEOs and boards to request an external effectiveness assessment of the full ORCM framework. See the Six Level ORCM Quality Assurance Framework for details.

c) ensure that annual business plans are in line with the approved risk appetite and incentives/disincentives are included in the compensation programmes to facilitate adherence to risk appetite;

**ORCM Enablers**: ORCM encourages application of formal risk/certainty assessment to corporate strategies and supporting objectives, including objectives that have potential to have a material impact on annual budgets. The OBJECTIVES REGISTER is populating using top strategic/value creation objectives and top value preservation objectives, including those linked to regulatory priorities. The probability of significant budget overages should receive specific attention during those assessments. Boards are encouraged to specifically request risk related information from the strategic planning group/executives, including the level of RISK/CERTAINTY ASSESSMENT RIGOUR applied to corporate strategies being considered, and those selected for implementation.

d) include an assessment of risk appetite in their strategic discussions including decisions regarding mergers, acquisitions, and growth in business lines or products;

**ORCM Enablers:** Board are encouraged to demand information on the amount of RISK/CERTAINTY ASSESSMENT RIGOUR that has been applied to all new strategies and proposed product/service lines and mergers and acquisitions, including information on the projected RESIDUAL RISK STATUS/CERTAINTY for these initiatives/related objectives and details on the top risks identified and how they will be addressed by the

company. See articles authored by Tim Leech for ETHICAL BOARDROOM and CONFERENCE BOARD DIRECTOR NOTES for more details on strategies to respond to escalating board oversight of risk expectations.

e) regularly review and monitor the actual risk profile and risk limits against the agreed levels (e.g. by business line, legal entity, product, risk category), including qualitative measures of conduct risk;

**ORCM Enablers:** ORCM assigns OWNER/SPONSORS to objectives deemed important enough to warrant formal risk assessment. Particular attention is paid to statutory/regulatory responsibilities linked to acceptable risk levels. Conduct risk is a "Risk Source" category that should be considered in all risk assessments. Boards receive regular reports on the OBJECTIVE CERTAINTY ratings linked to all objectives in the OBJECTIVES REGISTER. 2nd line risk personnel and 3rd line Internal Audit are expected to provide regular reports to the board on the reliability and sufficiency of risk status information the board is receiving.

f) discuss and monitor to ensure appropriate action is taken regarding "breaches" in risk limits;

**ORCM Enablers:** for objectives that have pre-determined risk limits specific attention is paid during the risk assessment to identify and assess the quality/reliability of MEASUREMENT/INDICATOR controls. This provides valuable information on the reliability of processes to detect and respond to breaches in risk limits**.** Details on the frequency and magnitude of breaches would be included as part of relevant risk assessments**.**

g) question senior management regarding activities outside the board-approved risk appetite statement, if any;

**ORCM Enablers:** ORCM frameworks can provide regular reports to the board on all objectives that have RESIDUAL RISK STATUS/CERTAINTY ratings outside of board approved risk appetite limits and cases where the OWNER/SPONSOR believes the current residual risk status/certainty is outside corporate risk appetite/tolerance. Both the risk function and internal audit are involved in providing reports on the reliability of information being provided to the board.

h) obtain an independent assessment (through internal assessors, third parties or both) of the design and effectiveness of the RAF and its alignment with supervisory expectations;

**ORCM Enablers**: the ORCM framework calls for regular reports from the risk group and internal audit on the design and effectiveness of the RAF, including conformance to applicable regulatory expectations. The framework also calls for explicit decisions on which objectives the company and/or board want independent assurance on and how much assurance. The ORCM six level quality assurance framework suggests CEOs and boards consider the need for a periodic expert external review of the ORCM framework. See the Six Level ORCM Framework paper for more details.

i) satisfy itself that there are mechanisms in place to ensure senior management can act in a timely manner to effectively manage, and where necessary mitigate, material adverse risk exposures, in particular those that are close to or exceed the approved risk appetite statement or risk limits;

**ORCM Enablers:** The RISK TREATMENT PRINCIPLES methodology used when completing CertaintyStatuslines on specific objectives linked to documented and undocumented risk limits encourage specific identification of controls/risk treatments to deal with situations identified as being outside of tolerance.

j) discuss with supervisors decisions regarding the establishment and ongoing monitoring of risk appetite as well as material changes in the current risk appetite levels, or regulatory expectations regarding risk appetite;

**ORCM Enablers:** When ORCM is used Boards should be well equipped to have robust discussions with regulatory supervisors on how the company and the board monitors acceptability of current risk appetite, and cases where there have been or will be material changes in appetite. Boards are encouraged to request and receive training on the ORCM framework, including new members joining the board.

k) ensure adequate resources and expertise are dedicated to risk management as well as internal audit in order to provide independent assurances to the board and senior management that they are operating within the approved RAF, including the use of third parties to supplement existing resources where appropriate; and

**ORCM Enablers:** the ORCM approach defines specific expectations for the C-Suite and board in terms of which value creation and value preservation objectives will be submitted to formal risk/certainty assessment, the target level of risk/certainty assessment rigour, whether independent assurance is required and from whom, and the target amount of independent assurance. Risk groups and internal audit are expected to regularly comment to the board on the sufficiency of the objectives included in the OBJECIVES REGISTER. This provides a vastly superior and defensible approach to determining the amount of risk and internal audit resources required. With other RAF approaches it is very difficult to determine the level of human resources required to staff risk and IA groups as there are no agreed outcomes/service level agreements. With the ORCM approach boards play an active role defining specific deliverables they want from risk groups and internal audit functions. In our experience, Boards of the majority of organizations today do not define with any clarity what they want as deliverables from risk functions or internal audit.

l) ensure risk management is supported by adequate and robust IT and MIS to enable identification, measurement, assessment and reporting of risk in a timely and accurate manner.

**ORCM Enablers:** A very robust set ORCM IT specifications has been developed for software to support the framework that specifically considers the primary regulatory requirements in force linked to monitoring of operational risk/ERM. The specifications include detailed requirements developed for financial service companies for loss event logging and analysis as well as real time monitoring of acceptability of residual risk status. ORCM software specifications are available at www.riskoversightsolutions.com

# 4.2 The chief executive officer should:

a) establish an appropriate risk appetite for the financial institution (in collaboration with the CRO and CFO) which is consistent with the institution's short- and long-term strategy, business and capital plans, risk capacity, as well as compensation programs, and aligns with supervisory expectations;

**ORCM Enablers:** in this framework CEOs are provided with concise reports on value creation and value preservation objectives which have been determined to have RESIDUAL RISK STATUS/CERTAINTY ratings outside of risk appetite/tolerance. Reports include concise information on the OBJECTIVE CERTAINTY RATINGS assigned to all objectives in the OBJECTIVES REGISTER. Situations where the OWNER/SPONSOR and/or company's position re acceptability of residual risk status/certainty is unclear, or where the risk group and/or IA function believe that it may be outside of entity risk appetite/tolerance are escalated up to the CEO and, where applicable, the board for review. Regulatory requirements are specifically considered when populating the company's OBJECTIVES REGISTER(S).

b) be accountable, together with the CRO, CFO, and business lines for the integrity of the RAF, including the timely identification and escalation of breaches in risk limits and of material risk exposures;

**ORCM Enabler:** ORCM policies define specific responsibilities for the CEO and the STRATEGY AND VALUE OVERSIGHT COMMITTEE. Overseeing the effectiveness of the ORCM framework is explicitly assigned. The management committees responsible for oversight of ORCM usually include C-suite executives. If the CEO is not on this Committee, the Committee is encouraged to engage the CEO in cases where significant risk acceptance decisions are required. This committee is specifically accountable for monitoring the integrity and sufficiency of the ORCM.

c) ensure, in conjunction with the CRO and CFO, that the risk appetite is appropriately translated into risk limits for business lines and legal entities and that business lines and legal entities incorporate risk appetite into their strategic and financial planning, decision-making processes and compensation decisions;

**ORCM Enablers:** As the ORCM produces information on the acceptability of RESIDUAL RISK STATUS/CERTAINTY linked to specific objectives C-Suite executives can elect to add additional risk treatments to bring the current RESIDUAL RISK STATUS/CERTAINTY back to acceptable levels. They can also decide to widen the number of documented risk limits via the entity's Risk Appetite Statement. The ORCM framework provides specific tools to help executives identify practical risk treatments available to reduce residual risk levels.

d) ensure that the institution-wide risk appetite statement is implemented by senior management through consistent risk appetite statements or specific risk limits for business lines and legal entities;

**ORCM Enabler**: The ORCM framework includes the use of documented risk appetite statements and encourages real time monitoring of the acceptability of RESIDUAL RISK STATUS/CERTAINTY linked to all value creation and value preservation objectives considered important/dangerous enough to warrant the expense of formal risk management processes and tools. Objectives that have documented risk appetite/tolerance limits are given particular attention.

e) provide leadership in communicating risk appetite to internal and external stakeholders so as to help embed appropriate risk taking into the financial institution's risk culture;

**ORCM Enablers:** CEOs are encouraged to play visible roles on STRATEGY AND VALUE OVERSIGHT COMMITTEE which oversees ORCM and defines target RISK/CERTAINTY ASSESSMENT RIGOUR LEVELS and target INDEPENDENT ASSURANCE levels for all objectives in the company's OBJECTIVES REGISTER. This includes the option of calling on OWNER/SPONSORS to personally explain the rationale behind specific risk acceptance decisions. When ORCM is in place companies are encouraged to follow the UK model of external representations by the company's board Chair to key stakeholders about the steps the company has taken to design and implement an effective ORCM. Samples of public disclosures on effectiveness of ORCM are available on request.

f) set the proper tone and example by empowering and supporting the CRO and CFO in their responsibilities, and effectively incorporating risk appetite into their decision-making processes;

**ORCM Enablers:** CEOs that take an active interest in reviewing objectives determined to have OBJECTIVE CERTAINTY RATINGS significantly outside of entity risk appetite/tolerance send a strong message to all objectives' OWNER/SPONSORS that ORCM is a framework that has the support and active participation of the CEO. CEOs are encouraged to play a leadership role on the company's STRATEGY AND VALUE OVERSIGHT COMMITTEE to emphasize the importance attached to identifying and monitoring the entity's risk appetite/tolerance.

g) ensure business lines and legal entities have appropriate processes in place to effectively identify, measure, monitor and report on the risk profile relative to established risk limits on a continual basis;

**ORCM Enablers**: CEOs are expected to take an active interest in which objectives are included in company's OBJECTIVES REGISTER and the effectiveness of the ORCM framework. CEOs are to be provided with regular reports from the risk group and internal audit on the effectiveness of the process, and any problems. CEOs are expected to respond to reports from the risk function and/or internal audit that OWNER/SPONSORS are not fulfilling risk management and reporting responsibilities assigned to them.

h) dedicate sufficient resources and expertise to risk management, internal audit and IT infrastructure to help provide effective oversight of adherence to the RAF;

**ORCM Enablers:** Risk groups and internal audit must communicate directly to the CEO and the company's STRATEGY AND VALUE OVERSIGHT COMMITTEE, a committee usually chaired by the CEO or his/her

designate, any resourcing shortfalls, including human resources and MIS support they believe they have in meeting the requirements for support defined in the company's OBJECTIVES REGISTER. A formal knowledge/skill profile for ORCM specialists is available on request.

i) act in a timely manner to ensure effective management, and where necessary mitigation, of material risk exposures, in particular those that are close to or exceed the approved risk appetite statement and/or risk limits; and

**ORCM Enablers:** The ORCM framework has an OBJECTIVE CERTAINTY RATING system that identifies situations where the attention of CEO and potentially the board is required immediately. This can include situations where risk limits are, or may be, materially exceeded. See definitions of OBJECTIVE CERTAINTY RATINGS for details of the escalation criteria.

j) establish a policy for notifying the board and the supervisor of serious breaches of risk limits and unexpected material risk exposures.

**ORCM Enablers:** The framework determines which OBJECTIVE CERTAINTY RATING level require immediate escalation to the board. The system can be modified to also include which objectives that have unacceptable risk/certainty ratings that may warrant notification of regulator/supervisors of breaches.

# 4.3 The chief risk officer should:

a) develop an appropriate risk appetite for the financial institution (in collaboration with the CEO and CFO) that meets the needs of the institution and aligns with supervisory expectations;

**ORCM Enablers:** development of entity Risk Appetite Statements (RAS) that define risk limits should be led by the CRO. These predefined limits should be specifically considered when defining and assessing objectives that the documented risk limits relate. Not all objectives will have predefined risk limits for all types of residual risk status/certainty situations. It simply isn't possible. Risk Appetite Statements should describe in detail the process used to determine and monitor the acceptability of RESIDUAL RISK STATUS/CERTAINTY linked to top value creation and value preservation objectives.

b) obtain the board's approval of the developed risk appetite and regularly report to the board on the financial institution's risk profile relative to risk appetite;

**ORCM Enablers:** In addition to seeking board approval for predefined Risk Appetite Statements, the CRO should play a lead role presenting the consolidated report on OBJECTIVE CERTAINTY STATUS linked to top value creation and preservation objectives and plans to bring unacceptable situations back in to entity appetite/tolerance. Objectives of particular interest to regulators and their current RESIDUAL RISK STATUS/CERTAINTY should receive particular attention. CROs are encourage to also include entity level synthesis of trends impacting current and projected residual risk levels with particular attention to "disruptive" risks that are challenging entity business models and strategies.

c) actively monitor the financial institution's risk profile relative to its risk appetite, strategy, business and capital plans, risk capacity, as well as compensation programs;

**ORCM Enablers:** the framework produces detailed snapshots of RESIDUAL RISK STATUS/CERTAINTY including situations considered to be outside of entity risk appetite/tolerance via OBJECTIVE CERTAINTY RATINGS (OCRs). OCRs can define the level of escalation up to and including the board. CROs play the lead role reviewing and synthesizing all reports on objectives included in the OBJECTIVES REGISTER and are well

equipped to provide big picture interpretation of current risk appetite/tolerance decisions and evolving risks, including disruptive risks with potential to change whole business sectors/business models.

d) establish a process for reporting on risk and on alignment (or otherwise) of risk appetite and risk profile with the institution's risk culture;

**ORCM Enabler:** ORCM specifically considers the need to align the ORCM methodology with the entity's culture and the training encourages facilitators and assessors specifically consider risks that may be a product of the entity's culture. This information is included in consolidated reports on risk/certainty status delivered by the CRO. See the ROS risk culture survey tool and recommended implementation strategies for more details.

e) ensure the integrity of risk measurement techniques and MIS that are used to monitor the financial institution's risk profile relative to its risk appetite;

**ORCM Enablers:** Specific attention needs to be paid to risks that can arise as a result of the use of models and risk indicator/measurement tools. These should receive specific and particular attention when they have potential to impact on specific objectives by workshop facilitators and risk analysts. Risk models that track and manage risk appetite decisions and reports may be of such critical importance that specific objectives should be defined and included in the entity's OBJECTIVES REGISTER.

f) establish and approve, in collaboration with the CEO and CFO, appropriate risk limits for business lines and legal entities that are prudent and consistent with the financial institution's risk appetite statement;

**ORCM Enablers:** CROs should actively and regularly provide input on the sufficiency and appropriateness of authority grids and risk appetite requirements that define limits on specific transaction types and specific risk related decisions. The CRO should also play a lead role ensuring that monitoring systems in place to ensure limits are complied with are robust and reliable.

g) independently monitor business line and legal entity risk limits and the financial institution's aggregate risk profile to ensure they remain consistent with the institution's risk appetite;

**ORCM Enablers:** CROs should be linked in to reporting systems designed to monitor and report on risk positions being taken/accepted. They should also pay particular attention to the risk status of assessments done on the reliability of risk monitoring systems. The risk group is expected to play an important role ensuring the reliability of all risk assessments completed by OWNER/SPONSORS. The Six Level Quality Assurance framework that accompanies ORCM is designed to provide assurance that risk/certainty status information being provided to the CEO and Board is sufficient and reliable.

h) act in a timely manner to ensure effective management, and where necessary mitigation, of material risk exposures, in particular those that are close to or exceed the approved risk appetite and/or risk limits; and

**ORCM Enablers**: CROs, in addition to monitoring the specific risk positions being accepted are expected to actively monitor the RESIDUAL RISK STATUS/CERTAINTY of all related objectives and report all situations where they believe management is accepting residual risk status/certainty positions outside of entity risk appetite/tolerance to the CEO and the Board. They should also work closely with OWNER/SPONSORs to identify practical and cost-effective risk treatments to address situations considered to be outside of risk appetite/tolerance.

i) escalate promptly to the board and CEO any material risk limit breach that places the financial institution at risk of exceeding its risk appetite, and in particular, of putting in danger the financial condition of the financial institution.

**ORCM Enabler:** CROs should ensure that the OBJECTIVE REGISTER includes objectives specifically linked to complying with risk limits considered material enough to warrant that level of attention. These objectives should be risk assessed at the target level of assessment rigour to identify any significant gaps in the risk

treatments in place. All RESIDUAL RISK STATUS/CERTAINTY RATINGS linked to risk levels should receive particular attention from the CRO.

# 4.4 The chief financial officer should:

a) develop an appropriate risk appetite for the financial institution (in collaboration with the CEO and CRO) which is consistent with the institution's short- and long-term strategy, business and capital plans, risk capacity, as well as compensation programs;

**ORCM Enablers:** CFOs play a primary role in the development of risk limits/risk appetite statements. Decisions are shaped by the organization's ability to withstand negative risk impacts and its ability to raise capital when required. In the ORCM framework the CFO is also expected to play a significant role reviewing significant risk acceptance decisions and the potential impacts. The CFO is also the OWNER/SPONSOR for multiple objectives key to financial goals, including objectives linked to reliable financial statements and entity solvency and liquidity.

b) incorporate risk appetite into the financial institution's compensation and decision-making processes (in collaboration with the CEO and CRO), including business planning, new products, mergers and acquisitions, and risk assessment and capital management processes;

**ORCM Enablers**: Because the objective centric approach starts with important end result objectives it is far better equipped to integrate the risk assessment information with compensation and decision making. Risk centric approaches are often not well integrated with compensation, and research indicates the information produced by "risk list" ERM is not considered key to decision making.

c) work effectively with the CRO and CEO to establish, monitor and report on adherence to applicable risk limits;

**ORCM Enablers:** The ORCM methodology recommends the CFO, CRO and CEO play important roles on the internal STRATEGY AND VALUE OVERSIGHT COMMITTEE deciding which objectives warrant formal risk assessment/management methods, who will be the OWNER/SPONSOR(S), the level of target risk/certainty assessment rigour, whether independent assurance is required and, if yes, the level of independent assurance. CFOs can play a lead role ensuring objectives linked to predefined risk appetite/tolerance levels receive particular attention.

d) act in a timely manner to ensure effective management, and where necessary mitigation, of material risk exposures, in particular those that are close to or exceed the approved risk appetite and/or risk limits within the CFO function; and

**ORCM Enablers:** As a member of the STRATEGY AND VALUE OVERSIGHT COMMITTEE objectives that are outside of entity risk appetite/tolerance are escalated and reporting frequencies on status can be increased to increase senior executive involvement. See definitions for OBJECTIVE CERTAINTY RATINGS.

e) escalate promptly to the CEO and the board (if appropriate) breaches in risk limits and material risk exposures that would put in danger the institution's financial condition.

**ORCM Enablers:** ORCM is designed to ensure that objectives with unacceptable RESIDUAL RISK STATUS/CERTAINTY RATINGS are automatically escalated. Material breaches of risk limits and material risk exposures would generally generate unacceptable OBJECTIVE CERTAINTY RATINGS. Risk groups and internal audit are required to monitor to the framework to ensure escalation of these situations is being escalated to the Board or relevant board committee.

# 4.5 Business line leaders and legal entity-level management should:

a) be accountable for effective management of the risk within their business unit and legal entity;

**ORCM Enablers:** the ORCM approach has the clearest line management accountability for managing risks linked to the entity's most important objectives. It has been designed to foster strong 1st LINE risk management capability. By formally assigning responsibility for assessing and reporting to OWNER/SPONSORS and tracking the status of how that responsibility is being discharged there is absolute clarity on accountability for reporting. STRATEGY AND VALUE OVERSIGHT COMMITTEES also define target RISK/CERTAINTY ASSESSMENT RIGOUR levels and make conscious decisions on the target level of independent assurance. The framework encourages Boards to have OWNER/SPONSORS present top value creation/value preservation objectives that have OBJECTIVE CERTAINTY RATINGS that indicate retained risk is outside of entity risk appetite/tolerance.

b) ensure alignment between the approved risk appetite and planning, compensation, and decision-making processes of the business unit and legal entity;

**ORCM Enablers:** Risk appetite limits are explicitly considered when objectives impacted are assessed. Objectives can be specifically designed/stated to support risk limits and full risk assessments completed including identifying relevant risk treatments and concerns with existing risk treatments. The link between objectives, risks, risk treatments, residual risk status/certainty, and performance is continuously tracked.

c) embed the risk appetite statement and risk limits into their activities so as to embed prudent risk taking into the institution's risk culture and day to day management of risk;

**ORCM Enablers:** see explanations above.

d) establish and actively monitor adherence to approved risk limits;

**ORCM Enablers:** The 9 nine category Risk Treatment Principles specifically looks for COMMITMENT controls that align with objective statements. When it is determined that there is a lack of accountability for a specific objective being risk assessed it is identified as a CONCERN UNRATED. Senior management must then make a conscious decision whether to accept it – CONCERN ACCEPTED or identify it as a CONCERN UNACCEPTABLE and put an ACTION PLAN in place to treat it. The nine risk treatment principles model is designed to quickly identify significant gaps in the risk treatment design. Specific attention is paid to the existence and reliability of INDICATOR/MEASUREMENT controls that should be in place to track risk limit status. INDICATOR/MEASUREMENT controls are classified as one of three "KEY" categories.

e) cooperate with the CRO and risk management function and not interfere with its independent duties;

**ORCM Enabler:** Owner/Sponsors are advised at the outset on the level of target RISK/CERTAINTY ASSESSMENT RIGOUR set by the STRATEGY AND VALUE OVERSIGHT COMMMITTEE. The risk group/2nd line are responsible for assisting and overseeing assessments generated by OWNER/SPONSORS. CROs are expected to report all situations where they are not receiving adequate support of the business lines and/or situations where the CRO believes that risk/certainty status reports are deficient and/or unreliable. See the SIX LEVEL QUALITY ASSURANCE FRAMEWORK for more details.

f) implement controls and processes to be able to effectively identify, monitor and report against allocated risk limits;

**ORCM Enablers:** the ORCM assessment methodology has been designed to specifically assess the reliability of frameworks in place to ensure conformance with specified risk limits. Depending on the level of target risk assessment rigour selected this assessment can be very sophisticated. See definitions of RISK/CERTAINTY ASSESSMENT RIGOUR for more details.

g) act in a timely manner to ensure effective management, and where necessary, mitigation of material risk exposures, in particular those that exceed or have the potential to exceed the approved risk appetite and/or risk limits; and

**ORCM Enablers:** the framework puts high importance identifying CONCERNS linked to specific risks and requires CONCERNS UNRATED identified during assessments be addressed on a timely basis by the OWNER/SPONSOR. When a decision is made accept a concern identified (CONCERN ACCEPTABLE) it is retained on file to allow the risk acceptance decision to be periodically revisited in light of new information/changes in risk appetite/tolerance.

h) escalate promptly breaches in risk limits and material risk exposures to the CRO and senior management in a timely manner.

**ORCM Enabler:** The RISK TREATMENT PRINCIPLES focus attention on MEASUREMEN/INDICATOR controls as a key category. This includes evaluating the reliability of reporting processes and whether information is being escalated as required.

# 4.6 Internal audit (or other independent assessor) should:

a) routinely include assessments of the RAF on an institution-wide basis as well as on an individual business line and legal entity basis;

**ORCM Enabler:** The standard ORCM corporate policy defines specific roles for management, risk groups, internal audit, CEO/C-suite and the Board. This approach has been labelled FIVE LINES OF ASSURANCE in papers contrasting OCERM to the more common THREE LINES OF DEFENSE. A key responsibility assigned to internal audit is to regularly report to the CEO and the board on the effectiveness of the ORCM framework. Internal auditors receive specific training on how to assess and report on the effectiveness of the ORCM framework. Details on the training that internal auditors receive on assessing the effectiveness of risk management processes/RAFs are available on request.

b) identify whether breaches in risk limits are being appropriately identified, escalated and reported, and report on the implementation of the RAF to the board and senior management as appropriate;

**ORCM Enabler:** this is considered an important subset of 4.6(a) and is given specific attention during the assessment of the ORCM framework.

c) independently assess periodically the design and effectiveness of the RAF and its alignment with supervisory expectations;

**ORCM Enabler:** A key decision when developing the “effectiveness” audit criteria used to evaluate RAFs is what they will be and where they are sourced from. The ORCM audit training recommends that the audit criteria used for the effectiveness assessment be drawn from relevant documented and undocumented regulatory expectations and effectiveness principles in ISO 31000 2018 and COSO ERM 2017. The principles in the FSB guidance in PRINCIPLES ON EFFECTIVENESS FOR RISK APPETITE FRAMEWORK are recommended as a primary starting point for internal audit assessments with particular attention being paid to assessing the risk culture that supports the ORCM framework. Local regulatory expectations that are an extension of FSB effectiveness criteria, or that conflict with the FSB RAF effectiveness principles, must be carefully considered.

ROS believes that, at the current time, most, if not all national financial regulatory expectations are less stringent than the FSB RAF 2013 effectiveness criteria.

d) assess the effectiveness of the implementation of the RAF, including linkage to organisational culture, as well as strategic and business planning, compensation, and decision-making processes;

**ORCM Enablers:** The ORCM framework defines specific steps that need to be followed to populate and define key criteria for objectives selected for inclusion in the OBJECTIVES REGISTER. ORCM methodology has been specifically and consciously designed to consider culture, and better integrate with strategic and business planning, compensation and decision-making processes. ORCM is far better positioned to achieve the FSB RAF effectiveness principles relative to risk centric/risk register based ERM methodologies.

e) assess the design and effectiveness of risk measurement techniques and MIS used to monitor the institution's risk profile in relation to its risk appetite;

**ORCM Enabler:** Once an organization builds a MIS to support ORCM drawing on specifications provided by ROS an entity will be well positioned to monitor real time the status of OBJECTIVE CERTAINTY RATINGS. If high levels of target RISK/CERTAINTY ASSESSMENT RIGOUR are selected this can include using technology to identify risk escalation triggers, link to risk likelihood and consequence information, run simulations, and more. Users are encouraged to integrate loss event tracking with the relevant objective(s) being assessed rather than to isolate the loss event data from the relevant objectives and risk assessments. Loss event data is a subset of MEASUREMENT/INDICATOR data and is specifically included in the RISK TREATMENT ELEMENTS.

f) report any material deficiencies in the RAF and on alignment (or otherwise) of risk appetite and risk profile with risk culture to the board and senior management in a timely manner; and

**ORCM Enablers:** See 4.6(c) for details.

g) evaluate the need to supplement its own independent assessment with expertise from third parties to provide a comprehensive independent view of the effectiveness of the RAF.

**ORCM Enablers:** See the ORCM Six Levels of Assurance for details. This requirement is Level 6 in the Six Levels of Assurance.

---

i