RISK OVERSIGHT SOLUTIONS

Owner/Sponsor Guide to CertaintyStatus*line*™

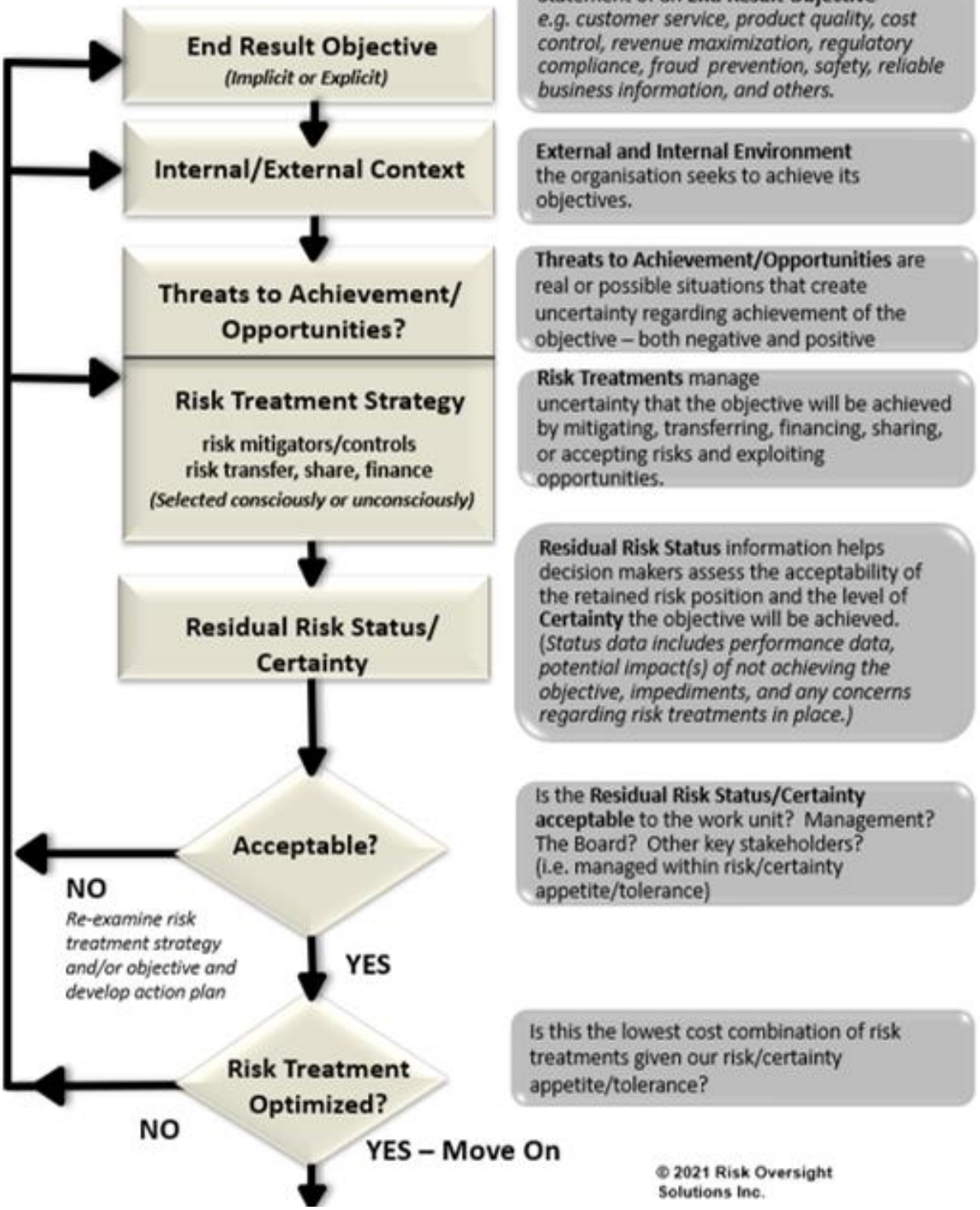
This document provides an introduction to the key steps required to complete a CertaintyStatus*line*™ strategy/objective centric risk assessment. Risk specialists and internal auditors are encouraged to take the full 11 module "Objective centric risk and certainty management" certificate course. Details on training available is available on ROS website TRAINING page.
https://riskoversightsolutions.com/training/

NOTE:

THIS GUIDE IS APPLIED ONCE THE "OBJECTIVE REGISTER" HAS BEEN POPULATED WITH AN ENTITY'S TOP STRATEGIC/VALUE CREATION AND VALUE PRESERVATION OBJECTIVES; AND THOSE OBJECTIVES HAVE BEEN ASSIGNED TO "OWNER/SPONSORS".

THIS IS A GUIDE TO ASSIST OWNER/SPONSORS COMPLETING STEP 4 DESCRIBED BELOW. RISK SPECIALISTS AND/OR INTERNAL AUDIT SHOULD ASSIST OWNER/SPONSORS.

CertaintyStatus*line*©



STEP 1: VALIDATE THE ASSIGNED OBJECTIVE

As an Owner/Sponsor you have been assigned responsibility for formally assessing and reporting on the residual risk status/certainty of achieving the objective(s) assigned to you. Your first step, which is an important step often overlooked, is to assess/agree that the objective assigned to you by the Strategy and Value Oversight Committee (the name we suggest) or similar body is:

- An end result objective (as opposed to an activity or task to be undertaken in support of one or more objectives), ideally with wording you agree with;
- Linked to the organization's top strategic/value creation objectives (e.g. entity purpose, revenue growth, cost reduction, share price, market share); or core value preservation objectives capable of significantly eroding entity value if not achieved (e.g. obeying important laws, reliable financial statements, safeguarding confidential information, business continuity, etc); is as specific as possible (e.g. "Our goal is to do well" versus "Our goal is to grow share price by 10% year over year");
- Set at the right level of granularity (e.g. minimize all unnecessary costs versus minimize unnecessary office cleaning costs) to pass the cost/benefit test; and
- Important enough/dangerous enough to warrant the incremental cost of including it in the Objectives Register and having management, perhaps with risk and/or internal audit assistance, complete a formal risk assessment and report results upwards to the Strategy and Value Oversight Committee or similar and the Board.

Formal risk assessment and assurance costs money and the decision to apply some level of formal documented risk assessment rigour (the definition of rigour per the Oxford dictionary is – "the quality of being extremely thorough and careful") should be made consciously and agreed with senior management, the Strategy and Value Oversight Committee that assigned you this objective, and potentially, if they are interested, the Board committee responsible for overseeing strategic planning and risk management frameworks. Boards of directors globally, particularly in financial service sector, have come under attack from regulators following the 2008 global financial crisis for not satisfying themselves that they are receiving enough reliable information on the true state of risk. Powerful institutional investors want to see evidence Boards are overseeing strategic planning and risk.

STEP 2: CONFIRM THE TARGET RISK ASSESSMENT RIGOUR RATING/THE AMOUNT OF TIME TO DEDICATE TO THE TASK

The number one objection senior management and work unit staff have to completing documented risk/certainty self-assessments is "We/I don't have time". This approach specifically recognizes that formal risk/certainty assessment (versus the informal variety that occurs daily at all levels of an organization) of an objective costs time and money. If an objective has been included in the

organization's Objective Register it means a decision has been taken by senior management and/or the Board of Directors and/or relevant regulators that some level of visible documented risk assessment is expected. As an Objective Owner/Sponsor you should confirm/agree with the assigned target Risk/Certainty Assessment Rigour ("RCAR") that defines how much effort/time/rigour the Strategy and Value Oversight Committee believe is warranted on the objective(s) assigned.

The minimum amount of Risk/Certainty Assessment Rigour allowed in this approach is one where the OWNER/SPONSOR(S) considers relevant risk and risk treatment information they are aware of; assigns an "OBJECTIVE CERTAINTY" rating; and writes a few paragraphs describing the logic. It can also include completing residual risk status/certainty information, including available performance/indicator data, impact data, and any impediments. This approach usually takes less than an hour. This is called INTUITIVE/EXPERIENTIAL, a relatively low level of risk/certainty assessment rigour. When a low level of rigour is used there is heavy reliance on the ability and integrity of an OWNER/SPONSOR to identify and assess significant risks to the objective and opportunities in their head without a formal process or documentation, and decide whether the current residual risk/certainty status (the level of risk/certainty after considering current risk treatments/controls used to manage risks) is within the entity's risk appetite/tolerance. This approach, when done with expert assistance, should not take more than a couple of hours.

NOTE: A large percentage of risk management done today in the world on strategic/value creation objectives is still done informally. It is important to note that even the INTUITIVE/EXPERIENTIAL level of rigour, the lowest level possible in this approach, is a higher level of assessment rigour for many objectives, particularly top value creation objectives, than many status quo approaches to strategic planning and risk management done by companies around the world. OWNER/SPONSORS are responsible for the OBJECTIVE CERTAINTY RATING assigned.

If it is decided that a higher level of risk assessment rigour is warranted for an objective, additional risk assessment rigour increments can range from an additional couple of hours, to what can be weeks, even months of work for the high rigour analytics and data analysis required by very high levels of risk assessment rigour.

If a low RAR option is specified assigning a OBJECTIVE CERTAINTY RATING ("OCR") of 0 indicates that the OWNER/SPONSOR(S) believe that the current residual risk/certainty status is within senior management and the board's risk appetite/tolerance. No additional risk treatments are warranted at the current time. If the OWNER/SPONSOR doesn't believe the current residual risk/certainty status is fully within the entity's appetite/tolerance, additional risk/certainty assessment steps may be undertaken, and efforts made to adjust residual risk/certainty status to an acceptable level. See STEP 8 in this guide for more details on OBJECTIVE CERTAINTY ratings.

STEP 3: CONFIRM THE PRIORITIZATION OF THE OBJECTIVE

If a decision has been made that an objective in the Objective Register warrants more formal documented risk/certainty assessment rigour than INTUITIVE/EXPERIENTIAL, usually the first step is to take some time to formally rate the objective on a number of important dimensions if this hasn't already been done by the Strategy and Value Oversight Committee. These dimensions include importance to the whole organization, importance to the business unit, potential to increase entity value, potential to erode entity value, current level of risk/certainty assessment rigour, target level of risk/certainty assessment rigour, the current performance rating (how well are we doing on this right now), and whether formal risk/certainty assessment linked to the objective is regulator mandated/expected (e.g. financial service regulators often expect to see evidence of risk assessment linked to anti-money laundering, market abuse, IT security and many other areas).

In an ideal world, this step would have occurred as part of the prioritization process to decide which objectives should be included in the organization's Objectives Register. At a minimum, the Objectives Register should include the entity's top strategic/value creation objectives, top value preservation/erosion objectives, and areas/objectives regulators require evidence of formal risk management. (e.g. financial statement reliability, compliance with certain laws, health and safety, IT security, business continuity, etc) The set of objectives that warrant inclusion in the OBJECTIVES REGISTER should be periodically revisited by the Strategy and Value Oversight Committee or equivalent, with careful consideration to costs/benefits and resources available. In cases where there is a risk group and/or an internal audit function, both groups should continually consider whether they believe one or more additional objectives should be added to the OBJECTIVES REGISTER. They can then make their recommendation with supporting logic to the Committee that decides which objectives will be included in the entity's OBJECTIVES REGISTER. Boards should also instruct management if they believe there are objectives that they want added to the Objectives Register.

STEP 4: IDENTIFY RISKS/THREATS TO ACHIEVEMENT

If a decision has been made to take the time to document and assess risks/threats to achievement (i.e. real or possible situations that create uncertainty regarding achievement of objective) and opportunities, the next step is to decide on how much risk/certainty assessment rigour will be applied. Traditional ERM programs and many internal audit methodologies often only utilize what is commonly referred to as the "brainstorming" approach to risk identification and assessment. This method relies heavily on the knowledge and experience of those participating. Used in isolation, particularly when done in a very short period of time such as annual internal audit planning or the annual risk register update meeting, brainstorming has regularly proven to be unreliable.

We recommend brainstorming be supplemented by a range of other risk identification techniques depending on the relative importance of the objective. Other viable risk identification methods include internet research, scenario modelling, visualization, flowcharting, inverse controls/risk treatments approach, statistical analysis, cause-of-failure approach, risk source model, Monte Carlo simulations, and others. For objectives involving life or death and objectives key to an entity's ongoing existence the rigour should be increased or a conscious decision made by senior management and the board to accept the additional risk that comes with not having invested much time/effort/resources formally identifying and assessing risks. (i.e. the risk of being viewed as not meeting regulator and/or stakeholder evolving risk oversight due diligence expectations) See Risk Oversight Solutions' TRAINING page on our website for details on all the training modules available.

STEP 5: ASSESS THE RISKS

Having identified some number of risks in Step 4, the next decision is how much time to commit to analyzing risks. A common step involves estimating risk likelihood and consequences. Different combinations of likelihood and consequence create what is commonly referred to as "risk levels". Risk levels in turn determine the level of management attention different risks warrant. If you are experiencing difficulty assigning risk likelihood/consequence ratings consider simply assigning a risk level. A table that determines risk levels from different likelihood/consequence combinations and the related management attention level definitions is shown below:

	Consequences				
Likelihood	extreme	very high	medium	low	negligible
almost certain	severe	severe	high	major	significant
likely	severe	high	major	significant	moderate
moderate	high	major	significant	moderate	low
unlikely	major	significant	moderate	low	trivial
rare	significant	moderate	low	trivial	trivial
SOURCE: *Guidelines for Managing Risk in the Australian Public Sector, #22 October 1996*					

RISK LEVEL DEFINITIONS

SEVERE – must be managed by senior management with a detailed plan
HIGH – detailed research and management planning required at senior levels
MAJOR – senior management attention is needed
SIGNIFICANT – management responsibility must be specified
MODERATE – manage by specific monitoring and response procedures
LOW – manage by routine procedures
TRIVIAL – unlikely to need specific application of resources

If time is limited, participants can simply estimate current effectiveness of the risk treatments in use without describing them and assign standard Red/Amber/Green ratings to each risk that indicate whether the current residual risk status, after considering risk treatments currently in place, is resulting in an acceptable level of residual risk. Definitions for standard "traffic light" risk status ratings for individual risks are as follows:

RED – current residual risk/certainty for the risk being considered is unacceptable. Additional risk treatments required

AMBER – current residual risk/certainty warrants monitoring. No additional risk treatments planned currently

GREEN – current residual risk/certainty is considered acceptable and within entity risk appetite/tolerance

Action items must, by definition, be developed and implemented for all RED rated risks. AMBER rated risks will be given increased scrutiny going forward but no risk treatment changes are considered necessary at the current time.

Careful consideration should be given to the quality of the inputs used to assess risks. The more "fact-based" the data is that supports likelihood/consequence/velocity and other risk assessment inputs, the more likely the assessment will result in sound resource allocation decisions.

STEP 6: IDENTIFY "RISK TREATMENTS"

If the decision is that additional formal risk assessment rigour is warranted, the next step is to document for some or all of the risks identified in STEP 5 the specific "risk treatments" in use/place. Risk treatments per ISO Guide 73, an internationally accepted terminology guide, setting out standard risk definitions can involve:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing risk in order to pursue an opportunity;
- removing the **risk source (3.5.1.2);**
- changing the **likelihood (3.6.1.1);**
- changing the **consequences (3.6.1.3);**
- sharing the risk with another party or parties [including contracts and **risk financing (3.8.1.4)]; and**
- retaining the risk by informed decision.

Users should consult the CertaintyStatus*line*™ Risk Treatment Principles and Risk Treatment Elements reference documents for illustrative risk mitigation/transfer/share risk treatments.

The risk treatment description should attempt to accurately describe what is actually done currently, as opposed to what policy or procedures indicate should be done. If there are any known concerns with a risk treatment, or the way it is applied in practice, these concerns should be documented initially as "Concern Unrated" and then later assigned either "Concern Acceptable" or "Concern Unacceptable". Action plans must be developed for all concerns unacceptable. Inaction on a concern that senior management and, in significant cases, the board of directors are aware of but not willing to act on or direct resources to address indicates the concern is, in fact, acceptable to management and the board.

Details on "OPPORTUNITIES" that could impact the likelihood/certainty of achieving the objective being assessed should also be documented.

STEP 7: DOCUMENT CURRENT "RESIDUAL RISK STATUS/CERTAINTY STATUS" DATA

Indicator Data– Any performance information available on how well the objective is being achieved.

Impediment Data – Any situations or problems that stand in the way of the objective owner/sponsor adjusting the risk treatment strategy and related residual risk status. These can relate to the lack of funds, cooperation of staff or other departments, training deficiencies, board/senior management attitudes, and others.

Concern Data – Any known or suspected problems or concerns with one or more risk treatments/controls in place to manage risk likelihood and/or consequence.
Note: This category includes what has traditionally been called control deficiencies.

Impact Data– How bad would it be if the objective was not met in whole or in part? How would the board, the organization, the staff, and others be impacted?

STEP 8: ASSIGN AN OBJECTIVE CERTAINTY RATING ("OCR") AND DOCUMENT/ASSESS RISK TOLERANCE

Deciding whether a particular residual risk/certainty status is, or is not acceptable to an OWNER/SPONSOR, senior management, and the board is difficult, but key to better resource allocation. Those making the decisions have to consider what resources available, competing priorities, risk/certainty status on other important value creation and preservation objectives, whether the

organization's current strategic focus is short or long term, impact on individual and group remuneration, priorities of investors, credit agencies and regulators, and much more. What this approach offers is substantially better information to make those complex decisions and conscious decisions on how much effort to dedicate to decision making.

A key goal of an effective risk management process is to strive to operate, continuously, to the extent possible, within senior management and board's risk appetite and tolerance. ISO definitions for the terms risk appetite and risk tolerance from ISO Guide 73 are noted below.

Risk appetite
The amount and type of risk that an organization is willing to pursue or retain.

Risk tolerance
An organization's or its stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives.

Source: ISO Guide 73: Risk Management – Vocabulary, 2009

Users are encouraged to reference the available supplemental guidance when assigning OCRs. Sample OBJECTIVE CERTAINTY definitions are listed below.

Objective Certainty
Fully acceptable level of certainty of achievement. Any significant concerns have been identified and shared upwards
Some management effort is required to increase certainty of achievement to an acceptable level.
Considerable management action is required to increase certainty of achievement to an acceptable level.
Significant analysis and corrective action by Senior Management and the Board is urgently required to increase certainty of achievement to an acceptable level.
Massive corrective action by Senior Management and the Board is required now to increase certainty of achievement to an acceptable level.

STEP 9: DEVELOP ACTION PLANS FOR UNACCEPTABLE CONCERNS

For risks assigned Red ratings where the current risk treatments are considered to be inadequate/flawed users should document a concern statement describing the retained risk status/certainty situation. Some concerns that are identified in the course of an assessment, including risks where there is no specific risk treatment, the risk treatment has flaws and/or viable risk treatments available are not being used, may be accepted by OWNER/SPONSORS subject only to the decision being consensus agreed to for significant issues by levels above them. (e.g. people are fully aware smoking cigarettes increases cancer risk of cancer and potentially death but may elect to continue smoking, remuneration system may cause staff to break the law to achieve objectives but senior management is OK with the risk)

For concerns deemed unacceptable users need to document action items detailing the new risk treatments that will be implemented and due dates to reduce the current residual risk/certainty status linked to the objective to O – fully within the entity's risk appetite/tolerance.

STEP 10: PERIODICALLY REVISIT THE RISK/CERTAINTY ASSESSMENT RIGOUR LEVEL, PERFORMANCE AND CRRR ASSIGNED

As an OWNER/SPONSOR of an objective you are responsible for periodically (ideally real time) reassessing Objective Certainty Rating(s) (OCRs) on the business objective(s) you have been assigned as new information emerges, including new information on priorities, risks, and performance information. The goal is to continuously assess whether the current residual risk/certainty status, including the state of action items to address risks to objectives deemed outside of risk appetite/tolerance, is being reliably reported to senior management and the board. In cases where risk functions and/or internal audit have been asked by the STRATEGY AND VALUE OVERSIGHT COMMITTEE to provide some level of independent assurance they will provide the OWNER/SPONSOR with feedback on the reliability of the risk/certainty assessment completed.