COSO ERM 2017 Principle	ROS Objective Centric ERM/IA Enabler
GOVERNANCE & CULTURE	
1. **Exercises Board Risk Oversight**—The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.	A "Risk Oversight Committee", usually with C-Suite participation, selects top value creation and value preservation objectives for inclusion in the organization's OBJECTIVES REGISTER and makes initial decisions on who will be the OWNER/SPONSOR for each objective, the target level of risk assessment rigour, level of independent assurance, if any, and if yes who will provide independent assurance. The board oversees that process and makes final decisions on objectives, rigour and independent assurance level/provider. The need to populate the OBJECTIVES REGISTER WITH top value creation objectives puts more visibility on the process management uses to define the organization's value creation strategy and supporting objectives. Because in this framework the board is expected to review and agree with what has been included in the OBJECTIVES REGISTER, it forces additional review of management's process to identify strategy and articulate supporting end result objectives. Supplemental Reference: Board Oversight of Long-Term Value Creation and Preservation: What needs to change? Tim Leech, Conference Board Director Notes Summer 2017
2. **Establishes Operating Structures**—The organization establishes operating structures in the pursuit of strategy and business objectives.	Operating structures play a key role identifying which executive is best positioned to be the OWNER/SPONSOR for top value creation and preservation objectives selected for inclusion in the organization's OBJECTIVES REGISTER. Supplemental Reference: ROS Sample Objective Centric Risk Management Policy
3. **Defines Desired Culture**—The organization defines the desired behaviors that characterize the entity's desired culture.	Decisions made on which objectives are included in the OBJECTIVES REGISTER, the accountability of each OWNER/SPONSOR to provide reliable/candid reports on residual risk/certainty status and the discipline provided by risk specialist groups and internal audit foster a culture of disclosure and candid discussion of top areas of exposure, – a key element of a healthy risk governance culture. Risk assessments and quality assurance reviews of risk assessments can

	reveal problems the current culture is/may be creating. Readers are encouraged to read the article in the reference link for a more in-depth discussion of board oversight of culture. Reference: Next Frontier for Boards: Oversight of Risk Culture, Parveen Gupta/Tim Leech, Conference Board Director Notes 2015
4. **Demonstrates Commitment to Core Values**—The organization demonstrates a commitment to the entity's core values.	Decisions made by management and the board on which objectives warrant inclusion in the OBJECTIVES REGISTER, the wording of those objectives, and decisions on acceptability of residual risk/certainty linked to core value objectives provide transparency on how much real commitment there is to stated core values and ESG objectives. In cases where a company claims to have a specific core values objective a competent risk/certainty assessment will show the actual level of corporate commitment to that objective.
5. **Attracts, Develops, and Retains Capable Individuals**—The organization is committed to building human capital in alignment with the strategy and business objectives.	The step of assigning an OWNER/SPONSOR to assess and report on the current risk status by itself forces increased alignment of human capital with strategy and objectives. On a more granular level a key step when assessing risks to specific top value creation and preservation objectives is answering a simple questions – Do we have the necessary skills and capabilities to support achievement of this objective? If the answer is no, or significant gaps are identified, it is identified as a concern for consideration by the OWNER/SPONSOR at the first level, C-Suite at the second level and, if necessary, the board of directors.
STRATEGY & OBJECTIVE- SETTING	
6. **Analyzes Business Context**—The organization considers potential effects of business context on risk profile.	The CertaintyStatusline assessment approach provides training on importance of business context and specifically requires consideration of the "internal and external context" as a core step in the risk/certainty assessment process. Owner/sponsors, facilitators and quality assurance reviewers should be trained to specifically identify and consider internal and external context when completing assessments. This step was first articulated in ISO 31000 2009 and has been amplified in COSO ERM 2017.

7. **Defines Risk Appetite**—The organization defines risk appetite in the context of creating, preserving, and realizing value.	The objective centric approach includes a key step often overlooked by other methods – conscious decisions on which objectives are considered important enough to warrant formal risk management processes. Part of that decision is careful consideration of the potential risk of not achieving a specific strategy/objective in whole or in part. If an objective is not included in the OBJECTIVES REGISTER and not identified for formal risk assessment there is significantly heightened risk the organization/C-Suite/Board may not be aware of the residual risk status/certainty and acceptability of the residual risk/certainty position linked to that objective.
8. **Evaluates Alternative Strategies**—The organization evaluates alternative strategies and potential impact on risk profile.	During the process of developing corporate strategy the planning team will be fully aware that strategy options that will be presented to the C-Suite and Board will need to be translated in to specific end result objectives. Objectives considered important enough will be included in the OBJECTIVES REGISTER initiating conscious decisions who will be the OWNER/SPONSOR, level of risk/certainty assessment rigour for that specific objective, level of independent assurance on the assessment, if any, and who, if anyone, will provide independent assurance on risk/certainty status reports for the board. It is important to note that "STRATEGY" is often a macro level expression of an objective/intent.
9. **Formulates Business Objectives**—The organization considers risk while establishing the business objectives at various levels that align and support strategy.	Not only does objective centric ERM foster greater focus on formulation and articulation of end result objectives that align with strategy, it also requires decisions be made which objectives are important enough to warrant the cost of formal risk/certainty assessment, the level of risk/certainty assessment rigour, the level of independent assurance on risk/certainty reports on selected objectives from OWNER/SPONSORS, if any, and who, if anyone, will provide independent assurance on risk/certainty status reports from OWNER/SPONSORS.
10. **Identifies Risk**—The organization identifies risk that impacts the performance of strategy and business objectives.	ROS training materials for risk specialists, workshop facilitators, and internal auditors include training on over 30 methods to identify and assess risks with specific coverage of top/recommended/most reliable risk identification methods. Heavy emphasis is put on the need for "fact based information" on risks

	being assessed, as opposed to guesses made from participants that may, or may not represent the real situation. Quality assurance reviews of primary assessments done by risk specialists and internal auditors or other specialists can provide increased confidence important risks have been identified and reliably assessed.
PERFORMANCE	
11. **Assesses Severity of Risk**—The organization assesses the severity of risk.	In the ROS objective centric approach risks are assessed on Likelihood and Consequence with a default five level system producing a "RISK LEVEL". The recommended 5X5 likelihood/consequence table that produces specific RISK LEVELs adjusts for high impact/low likelihood risks that are sometime ignored in other approaches. The default risk level terms were developed in Australia in the mid-1990s. The RISK LEVEL of a specific risk defines the level/amount of management attention it should receive.
12. **Prioritizes Risks**—The organization prioritizes risks as a basis for selecting responses to risks.	Risks are prioritized by RISK LEVEL (see above) and a simple initial estimate of RED/AMBER/GREEN assigned for each risk. It is important to note that before risks are prioritized objectives have been prioritized during the process to populate the OBJECTIVES REGISTER, including defining value creation/erosion potential, target risk/certainty assessment rigour and target independent assurance levels.
13. **Implements Risk Responses**—The organization identifies and selects risk responses.	The methodology provides an easy to understand and use 9 category RISK TREATMENT PRINCIPLES model consisting of over 100 specific risk treatment elements to assist users. Simple, easy to understand "Trigger Questions" provide a succinct explanation of the full range of risk treatment/response elements that can be used to treat/respond to risks. These include risk transfer/risk finance/risk share/risk avoid as well as the more common risk mitigate, often referred to as "controls".
14. Develops Portfolio View—The organization develops and evaluates a portfolio view of risk.	By assembling a universe of the top value creation and value preservation objectives it allows the C-Suite and Board to see where high levels of retained risk exist on specific objectives and current state of action plans underway and the overall retained risk position across all the top objectives. One of the most important

	decisions in risk management is RESOURCE ALLOCATION. The objective centric approach provides specific actionable information for senior executives and boards on retained risk status on all objectives in the OBJECTIVES REGISTER that helps senior management and the board make better resource allocation decisions.
REVIEW & REVISION	
15. **Assesses Substantial Change**—The organization identifies and assesses changes that may substantially affect strategy and business objectives.	By assigning an OWNER/SPONSOR to each objective included in the OBJECTIVES REGISTER, and specifically assigning responsibility to monitor and report on the COMPOSITE RESIDUAL RISK/CERTAINTY STATUS for those objectives it increases the likelihood major changes in internal/external context, risks, risk treatment/responses and performance on the objective will be noted by the OWNER/SPONSOR and significant changes in COMPOSITE RESIDUAL RISK/CERTAINTY STATUS reported upward, particularly when the changes are potentially negative/dangerous.
16. **Reviews Risk and Performance**—The organization reviews entity performance and considers risk.	The CertaintyStatusline assessment approach specifically requires consideration of current performance information when deciding which objectives warrant inclusion in the OBJECTIVES REGISTER, and recording of best available performance information each time RESIDUAL RISK/Certainty STATUS information in individual CertaintyStatusline assessments are refreshed/updated. The link between risks, risk treatment/responses, and current performance for each objective assessed is visible and specifically tracked. Few other risk assessment methods we are aware of make this explicit link between objectives, risk assessment information, and related performance on the objective. This allows management to see how performance changes when risk treatment/response design is changed.
17. **Pursues Improvement in Enterprise Risk Management**—The organization pursues improvement of enterprise risk management.	In the objective centric approach we promote a key responsibility of specialist risk groups and internal audit is to continually evaluate the entire ERM framework, provide reports on framework performance, and recommendations for improvement to senior management and the board. The board of directors has specific responsibility to oversee the process and demand

	changes if they do not believe the framework is providing the board with materially reliable information on the true state of residual risk/certainty of achieving objectives. ROS offers a sample Strategy and Value Oversight Policy that details the roles of all the assurance players, including the board, CEO, STRATEGY AND RISK OVERSIGHT COMMITTEE, business units, risk specialists and internal audit.
INFORMATION, COMMUNICATION & REPORTING	
18. **Leverages Information Systems**—The organization leverages the entity's information and technology systems to support enterprise risk management.	The CertaintyStatusline assessment approach encourages users to seek fact-based information on risk likelihood, risk consequence, risk velocity, key risk indicators, and past and current performance on the objectives being assessed. When software is used data can be "wired" to the risk assessment to provide real time information, escalator triggers/alarms, and status alerts for OWNER/SPONSORs, senior management and boards. Tim Leech, CEO of Risk Oversight Solutions designed and successfully launched CARDmap software, the world's first integrated objective centric risk and assurance software in 1997. He sold that company in 2004. He is currently actively seeking software vendors now that want to offer objective centric/strong 1st line risk management software.
19. **Communicates Risk Information**—The organization uses communication channels to support enterprise risk management.	By assigning each objective that is considered important enough/material enough to warrant the cost of formal risk/certainty assessment to an OWNER/SPONSOR, and assigning formal responsibility to report on status it forces/facilitates communication about retained risk/certainty status. On objectives where an independent assurance provider has been assigned, a key role is to report on the timeliness and reliability of residual risk/certainty status reports from OWNER/SPONSORS to senior management and the board.
20. R**eports on Risk, Culture, and Performance**—The organization reports on risk, culture, and performance at multiple levels and across the entity.	The OBJECTIVES REGISTER and CertaintyStatusline risk assessment approach provides a practical platform to report on residual risk/certainty status and performance. When culture is considered to be a risk to a specific objective OWNER/SPONSORS are encouraged to identify and assess it as a potential

	risk. Specialist risk groups, where one exists, are expected to provide reports on the overall effectiveness and reliability of the ERM framework. Internal audit, pursuant to IIA IPPF professional standard 2120 should be providing regular quality assurance reports to senior management and the board on the effectiveness of the entity's risk management framework.