Enterprise Risk Management Model

The Enterprise Risk Management (ERM) Model is a system used to analyze the cost and benefit of addressing risks inherent in the work performed by the Department of Energy. This system measures risk using a combination of qualitative and quantitative methods to set a standard method for analyzing risk across the many functions within the department. Risks generally fall within five categories regardless of the subject matter of the subsystem. These categories are (1) risks to people, (2) risks that hinder mission accomplishment, (3) risks to departmental physical assets, (4) financial risks, and (5) risks that destroy credibility and trust by the customers, stakeholders, and the general public. A comparison of rough costs estimates for potential risks and the controls that address them can help the Department ensure that all risks are sufficiently addressed through acceptance, monitoring, mitigation, or avoidance. This system also ensures that controls are not applied when the cost of the controls exceeds the cost of risk acceptance.

Risk Analysis and Determination of Controls for Incorporation into Directives

The preliminary review of each subsystem begins with a risk analysis performed by a team of senior level representatives of the Department. The team should be comprised of senior level representatives chosen by members of the Directives Review Board (DRB) who represent the Undersecretaries, the NLDC, and the subsystem under review. A facilitator can be made available from MA's Office of Information Resources. This team will perform the risk analysis using the following five steps.

1. **Identify Risks** – List all possible events that could occur in a subsystem if there are no controls. Once risks are identified, combine like risks according to the following key areas impacted by the risks: people, mission, physical assets, financial assets, and customer/stakeholder trust.
2. **Evaluate Risks** – Rate risks according to probability and impact.
3. **Identify Existing Risk Mitigation** – List all controls that would exist without DOE subsystem-specific controls.
4. **Identify New Risk Controls** –Where there is a significant or extreme risk rating, list gaps between existing risks and existing controls. For risks rated moderate, proposed controls must demonstrate a clear benefit according to a CD-0 (approval of a mission need) level cost-benefit analysis.
5. **Risk Register** – Create a register that documents the results of the risk evaluation, including the events, probabilities, impacts, and risk management strategy.

After the rough proposed list of controls has been generated, it is attached to a Justification Memorandum (JM) and sent to the DRB for review and approval.

While the subject matter experts will provide input and advice throughout the process, it is ultimately the responsibility of the team to ensure the proposed list of controls adhere to the principles of the Enterprise Risk Management Model. This means that controls must be based

on the acceptance, mitigation or avoidance of risks and that all proposed controls should be considered according to their potential costs and benefits.

Requirements Document Preparation

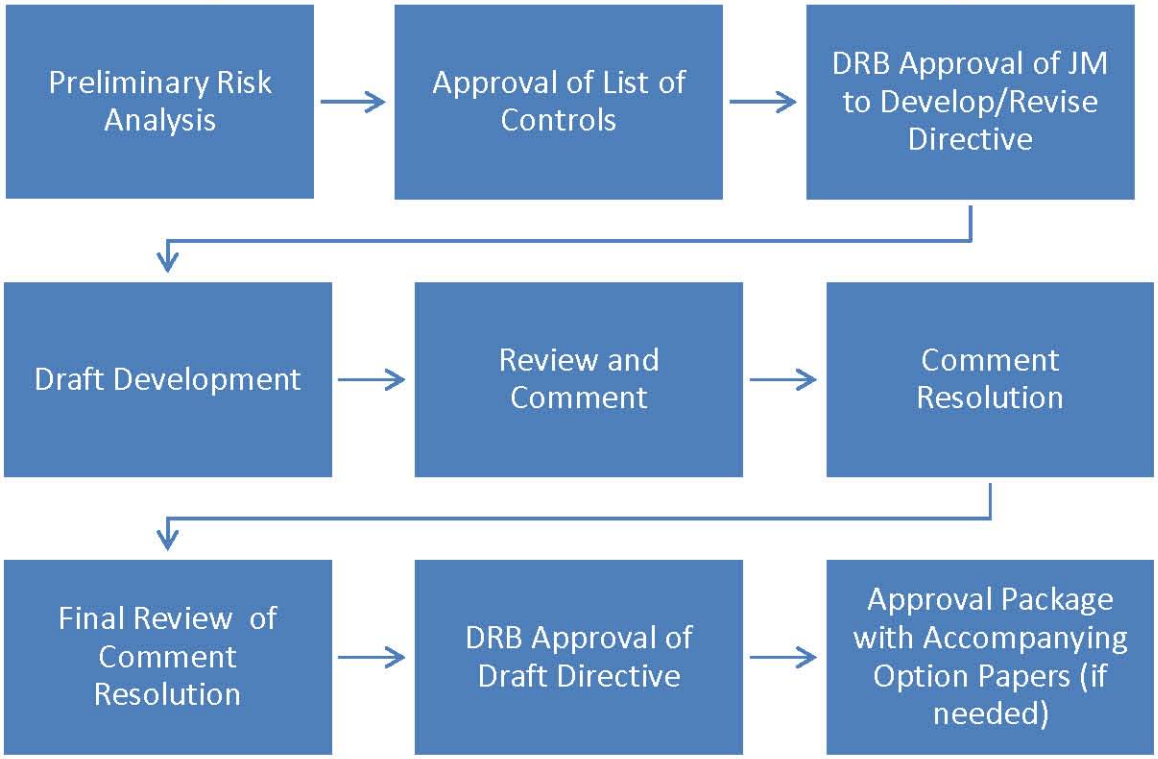
Once the JM is approved, the team ensures a draft requirements document codifies the proposed list of controls in an efficient and effective manner. The draft is then submitted for corporate-wide review through RevCom. All comments are reviewed by the team and presented to the DRB.

The DRB determines which comments should be incorporated into the second draft. The team is responsible for incorporating these edits into a redline draft. The redline is then posted online and notifications are sent out to all Directive Points of Contact (DPCs). Within the notification are instructions to submit any concerns or comments to their representative of the DRB, through their lead DPC. It is ultimately at the DRB member's discretion to submit concerns or comments to the DRB during the final review process.

Document Approval

If no concerns are received prior to the DRB meeting, a formal approval package is prepared for the Deputy Secretary's (or Director, Office of Management's for Guides) approval; the package will comprise the risk register, the JM, the comments disposition, and the final version.

Process for Subsystem Review under the Enterprise Risk Management Model



Process for Review of Subsystems Already within the ERM

Future revisions to requirements documents can be initiated by any Program Secretarial Officers through the DRB. Any request should explicitly state the reason for the proposed review and should be based on at least one of the following reasons; (1) a change in risks, (2) a change in controls outside of the subsystem, and/or (3) a potential cost savings based on a change to subsystem-specific controls. The DRB may choose to request an ERM Team be established to address these risks and determine whether a proposed modification to the list of controls is needed. All requirements documents should be reviewed, at a minimum every four years, for continued relevance.