Internal Risk Policy Essentials – Ensuring Success & Avoiding Pitfalls

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Commerce under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM23-0026

Ensuring Success & Avoiding Pitfalls

CERT's analysis of lessons learned from numerous internal risk program policies revealed some common pitfalls.

- Policies should be *specific* enough to avoid ambiguity, misinterpretation, conflict
- Policies should be *high-level* enough that they do not need to be modified more often than once every two years
- Policies should *incorporate* (authorize) other internal risk program documents by reference (e.g., CONOPS, Incident Response Plan, SOPs)

Some Essential Items for an IRP Policy (*being specific*)

A declarative statement that the program is established, along with some rationale

The authority of the IRP (*collect?, analyze?, coordinate?, respond?*)

Applicability of the InTP (*everyone? a subset?*)

Governance of the InTP (*Designated Senior Official, NEP, SC, Program Manager, Stakeholders*)

Roles and responsibilities of governance structure (*who and what*)

Scope of the IRP (*types of threats, what assets are covered*)

Definitions section (*what is a trusted insider, what is an internal risk threat*)

Examples of Incorporating IRP Documents by Reference

CONOPS – "The IRP program manager, in conjunction with the Standing Committee, will create a Concept of Operations (CONOPS) document"

Incident Response Plan – "The Designated Senior Official shall ensure there is an approved Incident Response Plan for the IRP"

SOPs – "The IRP program manager shall establish SOPs as necessary to codify the daily activities of the IRP"