



Internal Risk Policy Essentials – Ensuring Success & Avoiding Pitfalls

Document Markings

Copyright 2023 Carnegie Mellon University.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

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”