

Cybersecurity Governance

Instructor: Governance is the processes of governing or administration, through responsibilities and practices with the goal of strategic direction to ensure objectives are achieved while managing risks, and verifying enterprise resources are used appropriately.

The objective of information security is to protect the confidentiality, integrity, and availability of information and resources - information security governance supports the implementation and management of an effective information security program. It also helps to demonstrate due care and due diligence through formal governing practices. The governance function that ensures compliance with policy and regulations, and addressed risk potential, could prevent or reduce penalties or negative consequence, in the event of a compromise.

Important outcomes of IS governance includes Strategic alignment, Risk management, Value delivery, Resource management, Performance management, Assurance integration.

Strong governance ensures alignment of information security with business objectives. This strategic alignment is considering the business culture and

structure to drive security requirements. Risk management is the wholistic approach to understanding the risk exposures, and mitigating or managing those risks. Value delivery is the impact or effect the security implementations are providing the organization; optimized investments. Solutions are adequately addressing risks or concerns. The resource management piece is efficiently and effectively using knowledge and infrastructure in to support business functions. Performance management is a measurement process, monitoring and meeting metrics to ensure objectives are achieved. And assurance Integration goes into making sure security controls and strategies are reviewed to ensure they're operating as intended, end-to-end.

There are established information technology governance frameworks to aid organizations with their compliance requirements and effectively manage and monitor security controls, technical issues, and organization risks.

To be effective, information security governance must be an integral, transparent part of enterprise governance. Enterprise governance is the organization operations as a whole, information security governance is a subset of that. Information security governance provides the strategic direction for security activities that supports business objectives. A strategy for

preservation is equally important as
a strategy for progress.

Notices

This material is based upon work funded and supported by the Department of Homeland Security 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 is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu. Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

DM18-0098