

Association for Information Systems

AIS Electronic Library (AISeL)

WISP 2020 Proceedings

Pre-ICIS Workshop on Information Security and
Privacy (SIGSEC)

12-12-2020

When Organizational Pressures Collide – Balancing Information Security Risk Management and Compliance

Darwin M. Rivera

Alvaro Arenas

Follow this and additional works at: <https://aisel.aisnet.org/wisp2020>

This material is brought to you by the Pre-ICIS Workshop on Information Security and Privacy (SIGSEC) at AIS Electronic Library (AISeL). It has been accepted for inclusion in WISP 2020 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

When Organizational Pressures Collide – Balancing Information Security Risk Management and Compliance

Darwin M. Rivera¹

Information Systems and Technology, IE Business School,
Madrid, Spain

Alvaro Arenas

Information Systems and Technology, IE Business School,
Madrid, Spain

ABSTRACT

Information Security Risk Management has found itself rising on the priority of organizations after the significant growth experienced by compliance activities in the last 20 years. This has led often to conflicts between the requirements of Information Security Risk Management and Compliance as said requirements could impact the same systems or compete from the same resources. This study identifies strategies and tactics that an organization might implement to address balancing the requirements of the two. Oliver (1991) Strategic Responses to Institutional Processes frame the strategies and tactics predicted by theory as well as inform what new insights can be derived from practice. A Children's Hospital system serves as a setting to explore how the Information Systems and Compliance organizations navigate balancing Information Security Risk Management and Compliance requirements. A new tactic is identified that supplements those predicted by theory where Information Security Risk Management and Compliance requirements balancing is supported by formalized governance structures and processes.

Keywords: Information Systems, Security, Risk Management, Compliance, regulated environments, information systems governance, Neo-Institutional theory

¹ Corresponding author. darwin.rivera@student.ie.edu +1 571 212 7942