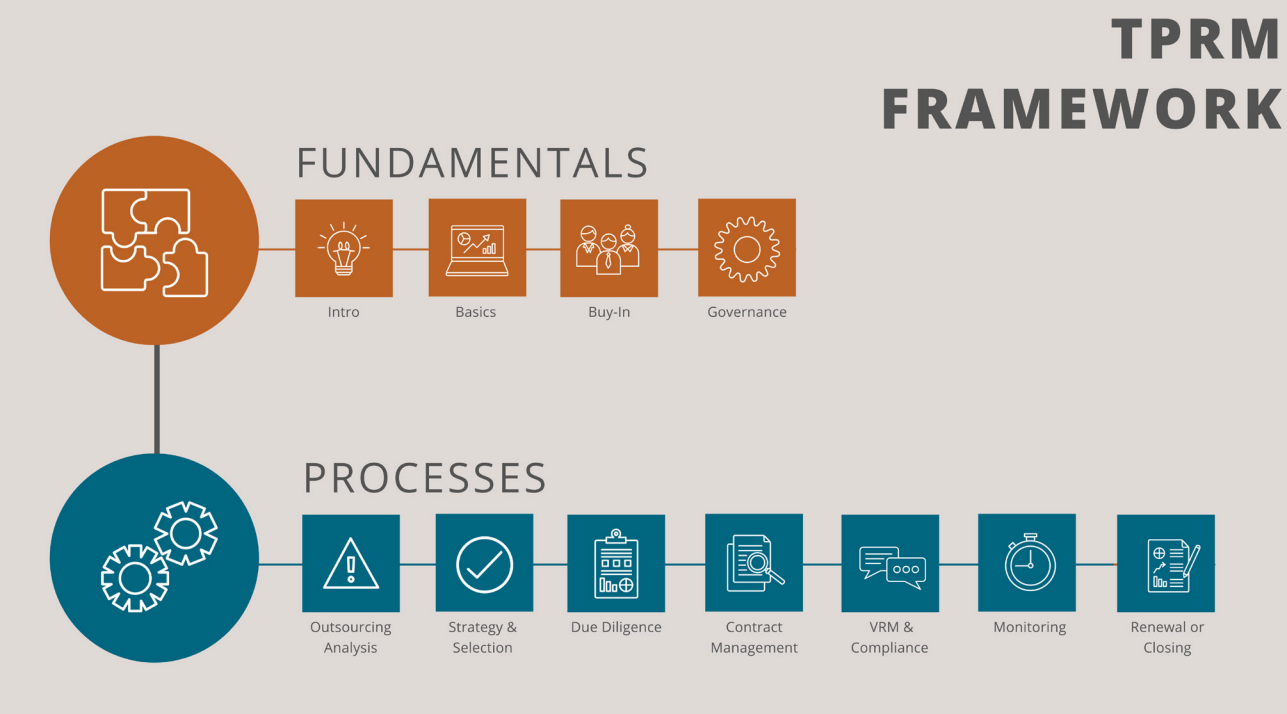
SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

TPRM FRAMEWORK FUNDAMENTALS

Introduction to the Framework

VERSION 1.0 | MAY 2019



Acknowledgments

The Shared Assessments Program's Third Party Risk Management (TPRM) Framework is designed to provide guidance for organizations seeking to develop, optimize and/or manage Third Party Risk by incorporating a wide range of techniques, including best practices, into their risk management programs. This publication is part of that Framework, and is one in a series of Shared Assessment Program resources on best practices in Third Party Risk Management. The Program's papers, articles and research studies are written and conducted by industry leaders — members of Shared Assessments Program Awareness Groups, The Santa Fe Group's partners, consultants, advisors and staff.

We'd like to thank the Shared Assessments Program's Steering Committee members and leaders who contributed to this effort:

- **Rocco Grillo**, Managing Director, Global Cyber Risk Services, Alvarez & Marsal
- **Emily Irving**, VP, RQA – Third Party Risk Management at BlackRock, Inc.
- **Shawn Malone**, Founder and CEO, Security Diligence, LLC
- **Tony Manley**, TPRM Professional
- **Glen Sgambati**, VP, Lead of Customer Success Executives at Early Warning Services, LLC

We would also like to acknowledge The Santa Fe Group, Shared Assessments Program subject matter experts and other staff who supported this effort:

- **Tom Garrubba**, Senior Director and CISO
- **Bob Jones**, Senior Advisor
- **Mike Jordan**, Senior Director
- **Charlie Miller**, Senior Vice President
- **Gary Roboff**, Senior Advisor, Lead Writer
- **Marya Roddis**, Vice President of Communications, Editor
- **Robin Slade**, Executive Vice President and Chief Operating Officer

Join the dialog with peer companies and learn how you can optimize your compliance programs while building a better understanding of what it takes to create a more risk sensitive environment in your organization.

About the Shared Assessments Program

The Shared Assessments Program has been setting the standard in third party risk management since 2005. Member-driven development of program resources helps organizations to effectively manage the critical components of the third party risk management lifecycle by creating efficiencies and lowering costs for conducting rigorous assessments of controls for cybersecurity, IT, privacy, data security and business resiliency. The Shared Assessments Program is managed by The Santa Fe Group (www.santa-fe-group.com), a strategic advisory company based in Santa Fe, New Mexico. For more information on Shared Assessments, please visit: https://www.sharedassessments.org.

Copyright © 2019
The Santa Fe Group,
Shared Assessments Program.
All Rights Reserved.

SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

Table of Contents

© 2019 The Santa Fe Group, Shared Assessments Program. All Rights Reserved.
For Member Use Only. Not for Dissemination.

SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

Introduction to the Framework

WHAT IS THE SHARED ASSESSMENTS TPRM FRAMEWORK?

The Shared Assessment Program's Third Party Risk Management (TPRM) Framework is designed to provide guidance for organizations seeking to develop, optimize and/or manage Third Party Risk by incorporating a wide range of best practices into their risk management program.

Although the Framework incorporates a wide range of best practice illustrations, it also:

- Raises awareness of the need for an enterprise-wide, holistic approach to third party risk management.
- Provides guidance about how to implement meaningful incremental improvements in TPRM practice maturity in organizations where resources may be constrained.
- Provides content designed for board members, C-level executives and both beginning and advanced practitioners.

The Shared Assessment Program's TPRM Framework:

- Fundamentals contains a short primer that introduces concepts that include inherent and residual risk; risk appetite statements and frameworks; risk tolerance metrics; and other foundational elements. TPRM Risk Basics introduces the importance of robust program governance and positive tone at the top to drive a strong organization-wide risk culture and management buy-in for resource allocation.
- Processes discusses program pre-requisites and process factors to be considered when building an organization's TPRM program, including factors relevant to making a decision about whether or not to outsource a specific business function or activity; the Third Party selection process and associated due diligence approaches; the contracting process; relationship management; contract compliance; ongoing monitoring (including continuous monitoring); and renewal, termination or closing of Third Party relationships.

© 2019 The Santa Fe Group, Shared Assessments Program. All Rights Reserved.
For Member Use Only. Not for Dissemination.

- A fully searchable online glossary is located at https://sharedassessments.org/glossary, which provides a listing of key terms and phrases used throughout the Third Party Risk Management framework.

WHY DO WE CARE ABOUT TPRM?

At a time when organizations are outsourcing more activities than ever before, TPRM has emerged as an important practice area within organizational risk management programs. That progress is happening in an environment where recent industry research suggests that only 40% of organizations have fully functioning TPRM programs (The Santa Fe Group, Shared Assessments Program and Protiviti, Inc., 2019).

While consumer data breach headlines continue unabated, it's not just personally identifiable consumer information that's increasingly at risk. In July 2018, a small Canadian contractor exposed tens of thousands of highly confidential records containing the sensitive intellectual property of virtually all U.S. based automakers. As the New York Times noted, that single incident illustrated "a problem confounding business: some of their biggest security risks come from their suppliers and contractors" (Cowley, New York Times, 2018).

Despite a necessary focus on information security within risk management, TPRM is a broader subject. The substance of TPRM encompasses all aspects of operational risk, including information security. A holistic approach to TPRM requires steps to reduce the risk of increased exposure to fraud through Third Party engagements. This approach involves consideration of geopolitical, geolocation and other critical concerns for organizational resiliency.

As the practice of Third Party Risk Management has evolved during the last 10 years, it has become increasingly evident that a fully developed TPRM framework could provide valuable assistance to organizations of all types as they seek to improve their outsourcing oversight processes.

THE CHANGING THREAT LANDSCAPE

Today's threat landscape has evolved in ways few might have predicted a decade ago and in ways that are making the risk management process increasingly complex.

© 2019 The Santa Fe Group, Shared Assessments Program. All Rights Reserved.
For Member Use Only. Not for Dissemination.

At the heart of the current TPRM landscape are:

1. Trust in the organization's risk management planning and processes;

2. Verification that the Third Party is meeting the Outsourcer's unique risk management requirements; and

3. Benchmarking of the Outsourcer's TPRM program effectiveness.

Business decisions cannot be made effectively in settings where TPRM program goals, risk metrics and the sources, devices and the data produced cannot be trusted. In the past, the consequences of not having TPRM process integrity could be severe. Today, the consequences can be catastrophic.

The complexity and gravity of the current landscape is composed of significant challenges:

SOCIOECONOMIC FORCES

- **The threat of industrial espionage and sabotage,** including intellectual property (IP) theft, has become a "mass phenomenon" in the manufacturing sector. The relevance of strong TPRM in CPG-settings is demonstrated in a current study, where seven out of 10 German manufacturing companies reported their organizations were victims of sabotage, data theft or espionage over the past two years. "Illegal knowledge and technology transfer, social engineering and also economic sabotage are not rare individual cases, but a mass phenomenon," stressed Thomas Haldenwang, Vice-President of the Federal Office for the Protection of the Constitution (Bitkom, 2018).
- **An uptick in geopolitical risk** from nationalistic regimes, resulting in a number of states requiring in-country data processing (e.g., MC/Visa in Russia had to move servers inside the Soviet Republic if they wanted to keep processing within those borders). Such restrictions make intrusion by the state a risk that is difficult, if not impossible, to control.
- **Quantum encryption research in Western countries is being threatened** by the operations of suppliers of key items for protection of critical infrastructure being restricted to nation states that have conflicting goals. Quantum-based encryption "device could break the encryption that protects digital information, putting at risk everything from the billions of dollars spent on e-commerce to national secrets stored in government databases" (Metz & Zhong, New York Times, 2018).
- **Increasing environmental/pollution/climate risks** have bred greater volatility across landscapes all over the world that affects business resiliency and continuity (e.g., extreme disruption in the form of hurricanes have created more chaos with greater frequency; severe droughts and

© 2019 The Santa Fe Group, Shared Assessments Program. All Rights Reserved.
For Member Use Only. Not for Dissemination.

the effects of how and where precipitation is delivered is becoming problematic for certain types of activities; severity of storms can place stress on production facilities on any type of activity involved in delivering services). In response, the need has grown for organizations to have increased site redundancies and communications that reach across possible outage points.

- **Pandemics remain a real threat** from diseases that are easily communicated, that are disabling to various degrees and for which drugs/vaccines are not always timely effective.
- **Reputational risks have increased** (e.g., ethical sourcing, trafficking, supply disruption), and supply disruptions can be difficult if not impossible to predict (e.g., Gatwick airport disruptions in December 2018 because of drone presence).

ARTIFICIAL INTELLIGENCE (AI) AND OTHER TECHNOLOGY CHALLENGES

- **AI can be worked against an organization, state, region, etc.,** but AI can also enhance security controls. With security increasingly relying on AI, not all organizations have an adequate focus on the potential impact of AI on TPRM risk management.
- **Internet of Things (IoT) device use has increased exponentially.** Surveys have shown that as much as 85% of businesses do not document the majority of their IoT devices, despite the fact that security incidents related to unsecured IoT devices can be catastrophic.

RETIREMENT OF KEY WORKFORCE COHORT GROUPS

- **Availability of skilled human resources is a growing risk factor.** Gaps in availability of talent and burnout are increasing threats, in part due both to the changing nature of population pyramids and geopolitical forces (e.g., when borders are sealed, talent pools are lost or compromised as limits placed on immigration and work visa issues). As the population skews toward older workers retiring, skills gaps are beginning to have a significant impact on risk management. The historical knowledge of organizations is being lost during this retirement process as well.

VARIABILITY OF DUE DILIGENCE IN CHANGING ECONOMIC CIRCUMSTANCES

- **The consequences of inadequate due diligence visibility are greater during an economic downturn** where impacts from a failing third party are more likely to be far greater than during a more stable economic environment. During periods of economic challenge, TPRM due diligence

© 2019 The Santa Fe Group, Shared Assessments Program. All Rights Reserved.
For Member Use Only. Not for Dissemination.

requirements can be significant, but may not be immediately visible (e.g., as part of mergers & acquisitions [M&A] activity, what happens when an organization goes bankrupt).

The Shared Assessments Third Party Risk Management Framework is designed to help organizations meet these and other challenges.

The Framework is designed to be tool agnostic. It does not focus solely on proprietary Shared Assessments Program Tools to the exclusion of other industry accepted approaches to TPRM. The Framework is designed to be a dynamic reference source and will be regularly modified and updated to reflect new risks, the changing regulatory and industry environments and risk management approaches.

© 2019 The Santa Fe Group, Shared Assessments Program. All Rights Reserved.
For Member Use Only. Not for Dissemination.