



FP CANADA RESPONSE TO FSRA CONSULTATION ON PROPOSED GUIDANCE ON IT RISK MANAGEMENT

Date: March 30, 2023

CONTENTS

FP Canada Response to FSRA Consultation on Proposed Guidance on IT Risk Management 1

 Contents 1

Introduction 2

Comments on the Proposed Guidance 2

Conclusion 3

INTRODUCTION

FP Canada™ is pleased to respond to the Financial Services Regulatory Authority of Ontario (FSRA) Consultation on Proposed Guidance on IT Risk Management (the proposed guidance).

Established in 1995, FP Canada is a national not-for-profit education, certification, and professional oversight organization working in the public interest. FP Canada is dedicated to championing better financial wellness for all Canadians by leading the advancement of professional financial planning across the country. There are about 17,000 CERTIFIED FINANCIAL PLANNER® professionals and about 1,900 QUALIFIED ASSOCIATE FINANCIAL PLANNER™ professionals as at December 31, 2022, who are held to FP Canada's rigorous professional and ethical standards – over 9,000 of whom are in Ontario.

FP Canada takes privacy protection and information security very seriously and supports FSRA's interpretation of risk, as well as the general principles and practices for effective IT risk management outlined in the consultation document.

Recognizing the critical role that information systems play in the business activities of FP Canada, FP Canada's Information Security Policy establishes and communicates, an enterprise-wide information security direction and cyber security risk management framework that aligns with applicable internal and external requirements necessary for the secure and reliable operation of FP Canada information systems. The Information Security Policy commits FP Canada to protect the confidentiality, integrity, and availability of its information and information systems, in an integrated manner, through an Information Security Management System (ISMS). The ISMS is a set of controls, policies and procedures designed to protect assets and sensitive data, and focuses on key elements such as risk governance, risk assessment, data/asset management, vulnerability management, access management, detection, and incident management.

As part of the application process for approval as a Credentialing Body (CB) under the Title Protection Framework, FP Canada outlined many of the ways that we manage information security and guard against cyber threats and breaches.

Our comments will focus specifically on the application of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) to CBs approved under the Title Protection Framework.

COMMENTS ON THE PROPOSED GUIDANCE

Under the proposed guidance, FSRA has stated that regulated entities “must comply with existing requirements related to IT risk and the protection of personal information,” and that “[t]his includes, but is not limited to, the requirements contained within PIPEDA.” Under the proposed guidance, FSRA has also set out a process for approved entities to notify it in the case of material IT risk incidents.

As there are already Provincial and Federal Commissions with jurisdiction over entities/bodies that are subject to PIPEDA and/or provincial privacy legislation, we do not believe that a new requirement from

FSRA to additionally report material breaches to FSRA via an open-ended email, enhances consumer protection in a space that is already well resourced and protected from a consumer standpoint. Federal and Provincial Privacy Commissions are best equipped to provide entities with advice and to escalate any concerns through their established systems and reporting requirements.

In addition, as part of FSRA's Annual Information Return (AIR) for CBs under the Title Protection Framework, each approved CB is required to disclose any security breaches involving information technology systems or electronic data that took place within the reporting period in which a "breach of security safeguards is defined in the Personal Information Protection and Electronic Documents (PIPEDA)." To add yet another additional layer to reporting to FSRA is redundant to FSRA's already established AIR process. We also do not believe FSRA is as well-positioned as the existing Federal and Provincial Privacy Commissions to manage privacy breaches.

It is therefore our view that FSRA's proposed oversight and disclosure requirements outside the AIR process adds an unnecessary layer of duplication. This proposal fails to appropriately recognize that all CBs under the Title Protection Framework are national in scope and are, therefore, already likely subject to both provincial and federal privacy legislation frameworks.

We recommend that the existing relationships and protection/reporting mechanisms, applicable between CBs and Federal and Provincial Privacy Commissions under their respective federal and provincial legislation, not be adapted, amended, or supplemented by FSRA. And, that CBs continue to disclose any material IT risk incidents through FSRA's AIR process.

CONCLUSION

FP Canada would like to thank FSRA for the opportunity to provide comment. We would welcome the opportunity to discuss our views with FSRA staff in greater detail.




Contact Details

FP CANADA™

902-375 University Avenue, Toronto, Ontario M5G 2J5

416.593.8587 | 1.800.305.9886 | fpcanada.ca

CFP®, CERTIFIED FINANCIAL PLANNER® and  are trademarks owned by Financial Planning Standards Board Ltd. (FPSB) and used under license. QAFF™, QUALIFIED ASSOCIATE FINANCIAL PLANNER™, QAFF and all other trademarks are those of FP Canada™.

© 2023 FP Canada™. All rights reserved.

