Summary of Feedback on Information Security Guideline

THEME	SUMMARY OF ISSUE/COMMENT	BCFSA RESPONSE
Need for an IS Guideline	There is agreement that information security is a material risk.	Agree
Structure	There is support for the organization of the IS Guideline.	Agree
Outsourcing	With respect to outsourcing, there are concerns about the ability for PRFI's to ensure third-party service providers meet IS Guideline expectations.	Many PRFIs outsource some aspect of their information management activities, particularly in the pension sector where outsourcing material activities is common. BCFSA expects that PRFIs will assess the information security capability of all third parties that manage information assets on its behalf, commensurate with the potential consequences of an information security incident affecting those assets. This assessment could include review of certificates and independent reports provided by third parties evidencing compliance with recognized standards (for example, International Organization for Standardization (ISO)). PRFIs, such as pension plan administrators, using "intragroup outsourcing" are subject to the same expectations as those outsourcing to service providers outside the group. Intragroup outsourcing is not necessarily less risky than outsourcing to an entity outside the "group". However, the notion of proportionality will be considered in intra-group outsourcing arrangements.
Proportionality	There is agreement that proportionality	In considering the application of this guideline BCFSA will consider the nature, scope,

	will be important when applying the guidelines, although there are questions about how BCFSA will determine, in practice, what that means.	complexity, and risk profiles of PRFIs. The sophistication of a PRFIs Information Security risk management program should reflect the PRFI's risk exposure and the sensitivity and significance of the data and information systems.
Equivalency	There are questions regarding the need for an Information Security Program to be structured exactly as described in the guideline.	The Guideline is principles based and is not meant to provide a prescriptive approach on how to achieve the guideline objectives. There are a variety of policies, procedures, practices, and control measures that an entity can institute to achieve the guideline objectives. Moreover, when reviewing a PRFI's information security program, BCFSA will consider the nature, scope, complexity, and risk profile of the PRFI. Where a PRFI already has an IS risk management program in place at the organizational level and a PRFI has been able to demonstrate that it has met the IS guideline expectations through existing policies, practices and procedures, BCFSA would deem the PRFI to have met those BCFSA's expectations on information security management .
Costs	There are concerns that meeting the expectations of the guideline would be costly particularly for smaller organizations.	While some submissions highlighted potential implementation costs that may be incurred, there were also comments that additional costs could be outweighed by the overall benefits provided. BCFSA understands the cost of meeting the expectations outlined in the guideline will vary by organization. Organizations with an advanced information security system may be able to meet these expectations with minimal additional requirements. Entities with minimal or no information security frameworks will require additional efforts to meet these expectations. However, in keeping with BCFSA's commitment to risk-based and proportionate supervision, the application of the guideline will depend on the nature, scope, systemic importance, complexity, and risk profile of the PRFI.

		However, BCFSA considers Information Security risks to be a material risk and sufficient resources should be allocated to address the risk.
Links to Privacy	There are some concerns with duplication of obligations related to privacy protection.	PRFIs are expected to meet all applicable legislation, regulations, and/or rules, as well as this guideline in their treatment of the PRFI's information. An information security incident may have privacy implications and, in that circumstance, PRFIs are expected to fulfill their reporting obligations.
Incident Reporting	There are concerns regarding the content, timing and disclosure of incident reports.	The expectation that a PRFI should inform the BCFSA of a major incident as soon as possible, and within 72 hours of a major incident provide BCFSA with an incident report, reflects standard practices used by other regulators. However, in response to concerns expressed regarding the potential burden of providing daily updates, the Guideline has been modified to allow the method and frequency of these updates to be established through discussions with the BCFSA. Regarding the content of the Incident Reports, BCFSA believes this information is necessary to understand the impacts of the incident on the PRFI's risk profile. For financial institutions, this information allows BCFSA to assess the potential impacts of the incident on the stability of the financial sector. BCFSA takes the management of information and the protection of privacy seriously and we are legally obligated to meet all the requirements of the Freedom of Information and Protection of Privacy Act (FOIPPA). FOIPPA prohibits the public release of some types of information, such as information that could harm the business interests of a third party and personal information (other than the applicant). FOIPPA also allows government agencies to

		withhold other types of information, such as policy advice or recommendations, legal advice, information submitted in confidence from another government, or information that could harm the ability of BCFSA to meet its mandate or fulfill its obligations. This means that all details that meet these exceptions will be removed from the information releases.
Use of a Guideline	There was a view that these expectations could be achieved using other tools such as through ERMs and BCPs.	While some of the specific expectations outlined in the IS guideline might be covered in an ERM or BCP, these documents may not cover all expectations of the IS guideline. As such, PRFIs are expected to review the IS guideline, identify any gaps in their existing policies and practices, and address the gaps identified, which may involve updating and aligning their policies and practices to the IS guideline.
Applicability to Pension Administrators	There were concerns about the relevance and applicability of this guideline to pension plan administrators.	BCFSA recognizes that many of the expectations outlined in the initial draft guideline were not appropriate for the pension sector. Therefore, the guideline was revised to provide pension sector specific expectations. All principles continue to apply to pension plan administrators. Also, some of the language used in the draft guideline may not be appropriate in the context of pension plan administrators. Therefore, BCFSA has adjusted some terminology in the guideline to make it more relevant to pension plan administrators.
Governance	There were issues raised about how to apply the governance principles, particularly with respect to pension plan administrators.	An area of particular concern to pension plan administrators related to the terminology used in the Governance principle. Consequently, BCFSA has redrafted this section to develop expectations specific to pension plan administrators.
Prescriptiveness	Some submissions stated that the guideline was too	BCFSA has issued a principles based IS guideline. BCFSA believes it has struck the appropriate balance between providing sufficient guidance to

	prescriptive while others requested further clarification.	enable PRFIs to mitigate risk without being overly prescriptive as there may be a range of controls to achieve a given information security objective. Specific implementation details are the responsibility of PRFIs, who may access the myriad available implementation resource such as NIST, CISA, CDN Cyber Security Centre, and CIS, to name a few.