Project Raven

Assessing financial sector cyber security and resilience

Exploring

ITEM	YES	NO	DEPT./ VENDOR	COMMENTS
1. Has your organization, at any time during the past 12 months, experienced a cyber-incident (hacking, intrusion, malware infection, fraud loss, breach of personal information, extortion, etc.) or experienced a lawsuit or other formal dispute (with either a private party or government agency) arising from a cyber-incident?				
2. Does every device in your organization have anti-virus and anti-malware software installed and do you keep this software up to date?				
3. Do you install all relevant security patches on every system in your environment (e.g., desktops, laptops, mobile devices, servers, firewalls, routers, switches, etc.)?				
4. Do any third parties have access to your network?				
5. Do third parties use multifactor authentication when connecting to your network?				

Adaptive generation of assessment questions

4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Yes	n/a
4X	Authentication of the identity of a user, process, and/or device must occur as a prerequisite to allowing system access	Partial	Feb-24
5	Network integrity is protected (e.g., network segregation, network segmentation)	Partial	Feb-24
6	Identities are proofed and bound to credentials and asserted in interactions	Yes	n/a
7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction	Yes	n/a

Answers suggested by AI using corporate docs.

AI-powered assistant for ways to improve

Solution design

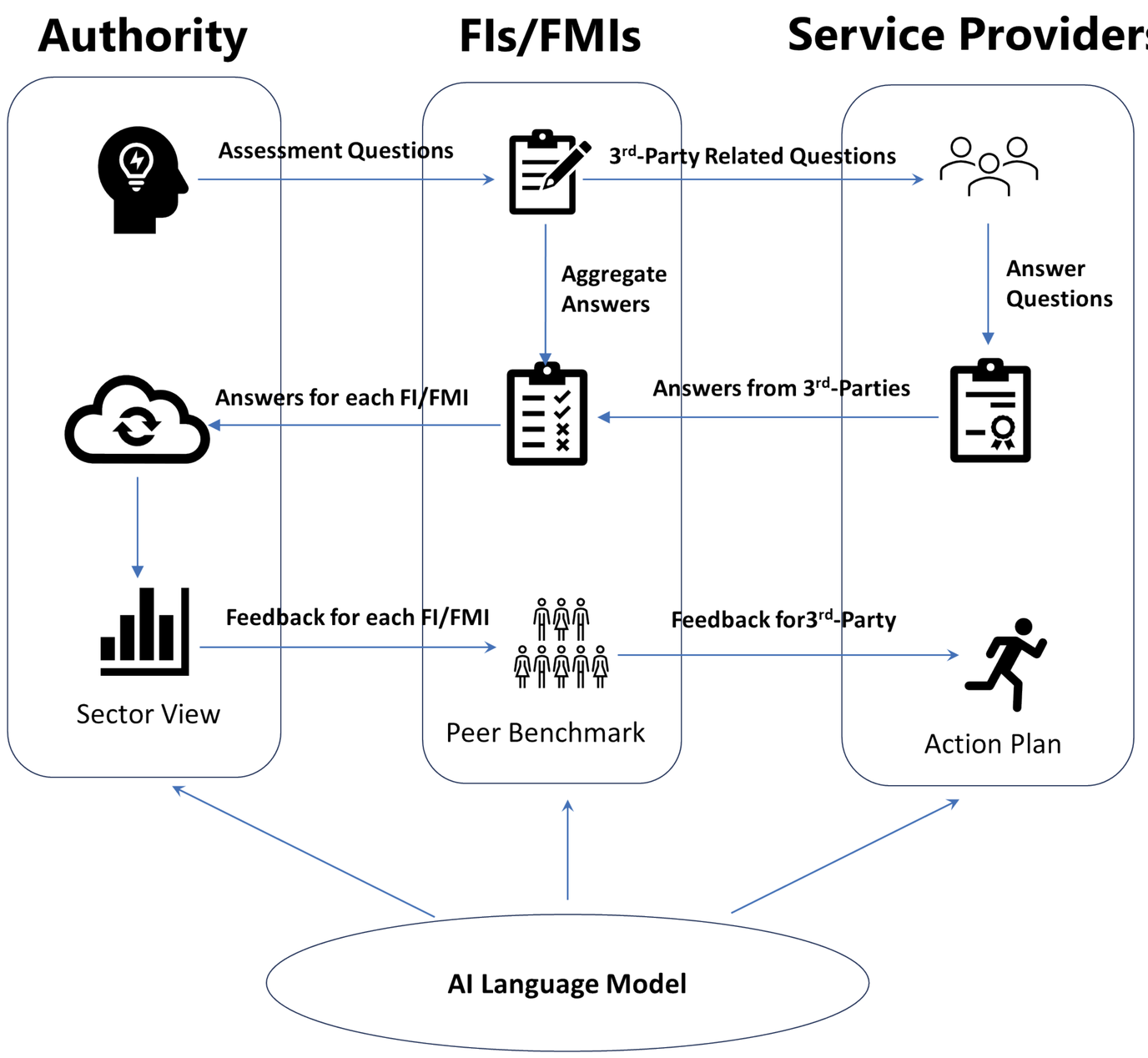
Build on existing practice
FSOR from Denmark, etc.

Reduce reporting burden
Introduce automation for operational efficiencies.

Low cost to run and support

Secure solution design and code

Go beyond a prototype
Deliver an MVP that is ready to deploy. Central banks can further enhance the solution.



Take-aways

1

Features

- Core baseline approach of questions, with room for jurisdictional specifics.
- Protection of sensitive information while providing peer benchmarking.

2

Benefits

- Increased automation in completing assessments.
- Shorter assessment cycle & higher response rate.
- Closing gaps sooner, improving the overall cyber posture.

3

Support for adoption

- Warranty support for first adopters.
- Full documentation.
- Operations managed by adopting authorities.

BIS Innovation Hub

Project Raven