Citi Internal Audit Innovation

Future Technology – FIRMA Conference

FIRMA Conference – Introduction

Marc Sabino

Citi | Innovation Chief Auditor

Why is the Power of Technology Important?

Assurance

Insights

Strategy

One Ecosystem

By rolling out a state-of-the-art audit platform, we've established a foundation to truly create "one ecosystem", including machine learning, natural language processing, bots, and AI

What is enabled by having one ecosystem?

By bringing more workflows and tasks into our platform, we are simplifying the way we work to derive greater efficiencies, and enhancing our ability to further digitize our data to derive meaningful insights, metrics and reporting

BENEFITS

- More time working in the platform
- Enhanced data and insights
- Simplification

Transformation Efforts

Artificial Intelligence

Scheduling

Methodology Streamline

Machine Learning

Utilizes Machine Learning (ML) and Natural Language Processing (NLP) to assess quality of controls, by evaluating the existence and quality of 5 Ws (Who, What, Where, When & Why) of control descriptions

What is enabled by this technology?

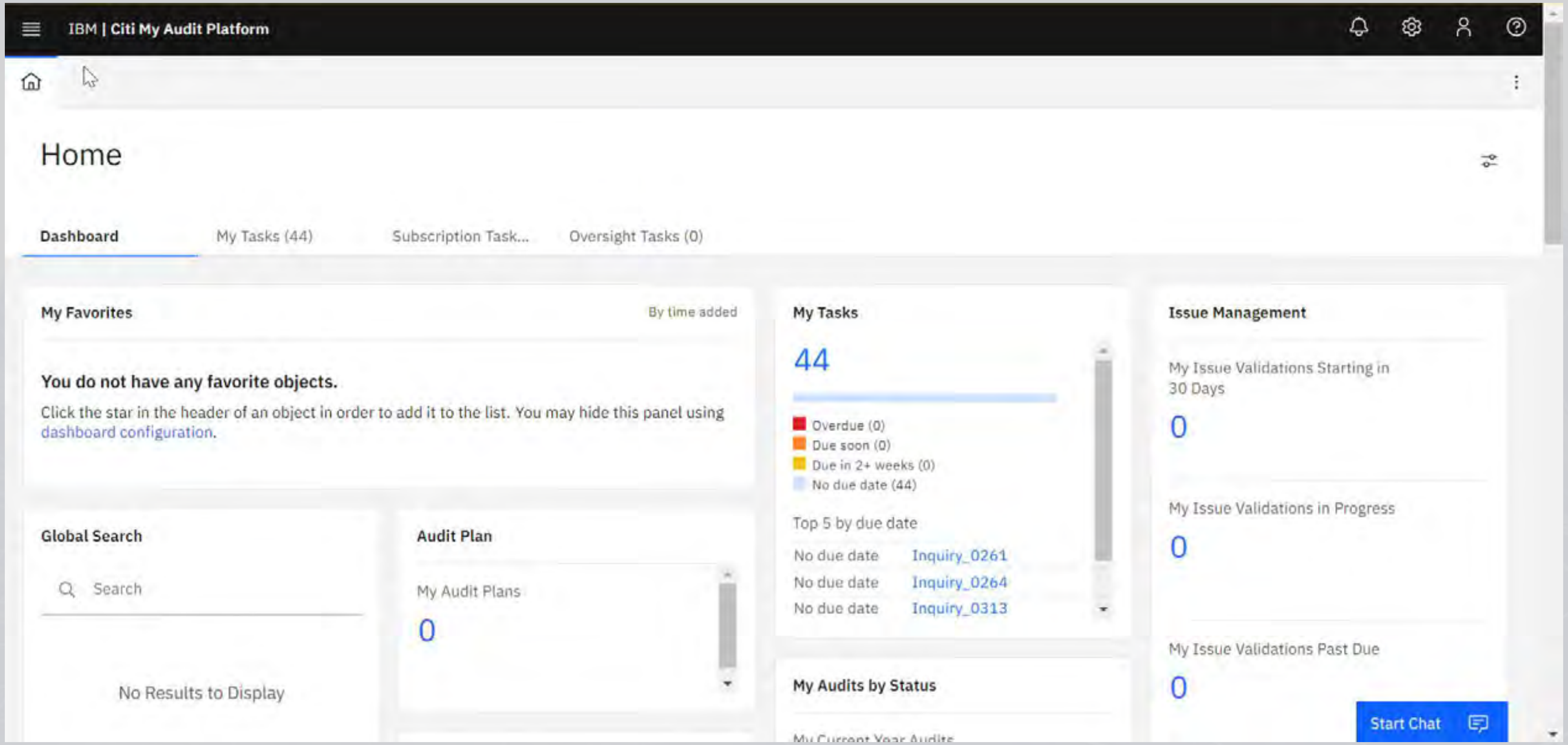
Well-written controls empower us to align with regulations and policies

BENEFITS

Empower us to align with regulations and polices

★★★ Enhanced quality

Consistency in tagging



IBM | Citi My Audit Platform

Home

My Favorites

By time added

You do not have any favorite objects.

Click the star in the header of an object in order to add it to the list. You may hide this panel using dashboard configuration.

My Tasks

44

🟥 Overdue (0)
🟧 Due soon (0)
🟨 Due in 2+ weeks (0)
No due date (44)

Top 5 by due date

No due date	Inquiry_0261
No due date	Inquiry_0264
No due date	Inquiry_0313

Issue Management

My Issue Validations Starting in 30 Days

0

My Issue Validations in Progress

0

My Issue Validations Past Due

0

Global Search

No Results to Display

Audit Plan

My Audit Plans

0

My Audits by Status

My Current Year Audits

Machine Learning – Chatbot (GRACE)

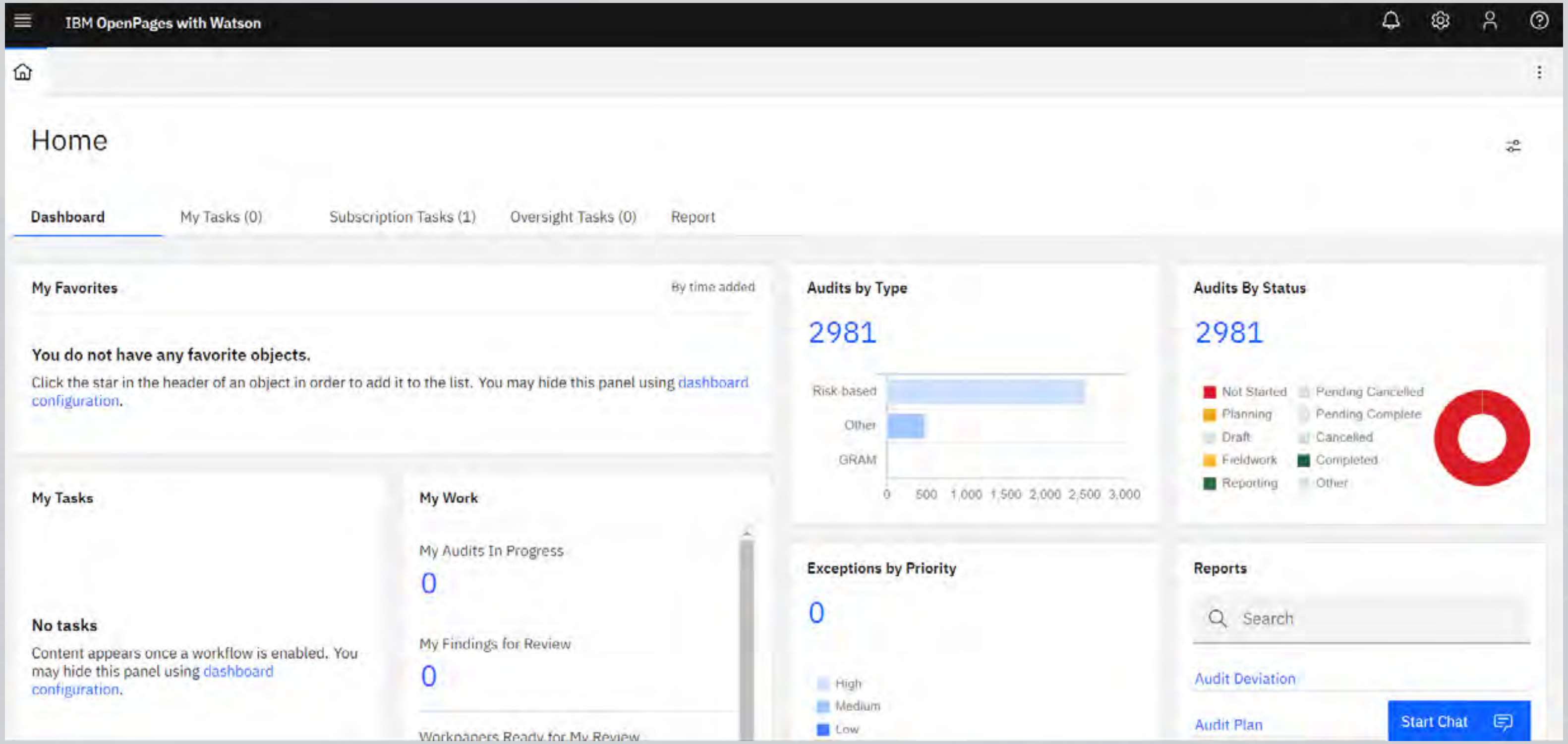
GRACE is our Internal Audit chatbot powered by IBM Watson technology. It leverages Machine Learning and Artificial Intelligence to understand questions and find relevant answers

What is enabled by this technology?

Self-service inquiry workflows by the audit teams provides information quickly and triages issues efficiently. The chatbot is constantly retrained in order to improve data quality and speed of responses.

BENEFITS

- Information at your Fingertips
- Added quality
- Enhanced Productivity
- Reduction in errors



You do not have any favorite objects.

Click the star in the header of an object in order to add it to the list. You may hide this panel using dashboard configuration.

No tasks

Content appears once a workflow is enabled. You may hide this panel using dashboard configuration.

Big Data and Connecting the Dots

Created with an initial volume of over 1TB of data to the Big Data EAP (Enterprise Architecture Process) environment for IA, this database is currently refreshed on a monthly basis

What is enabled by this technology?

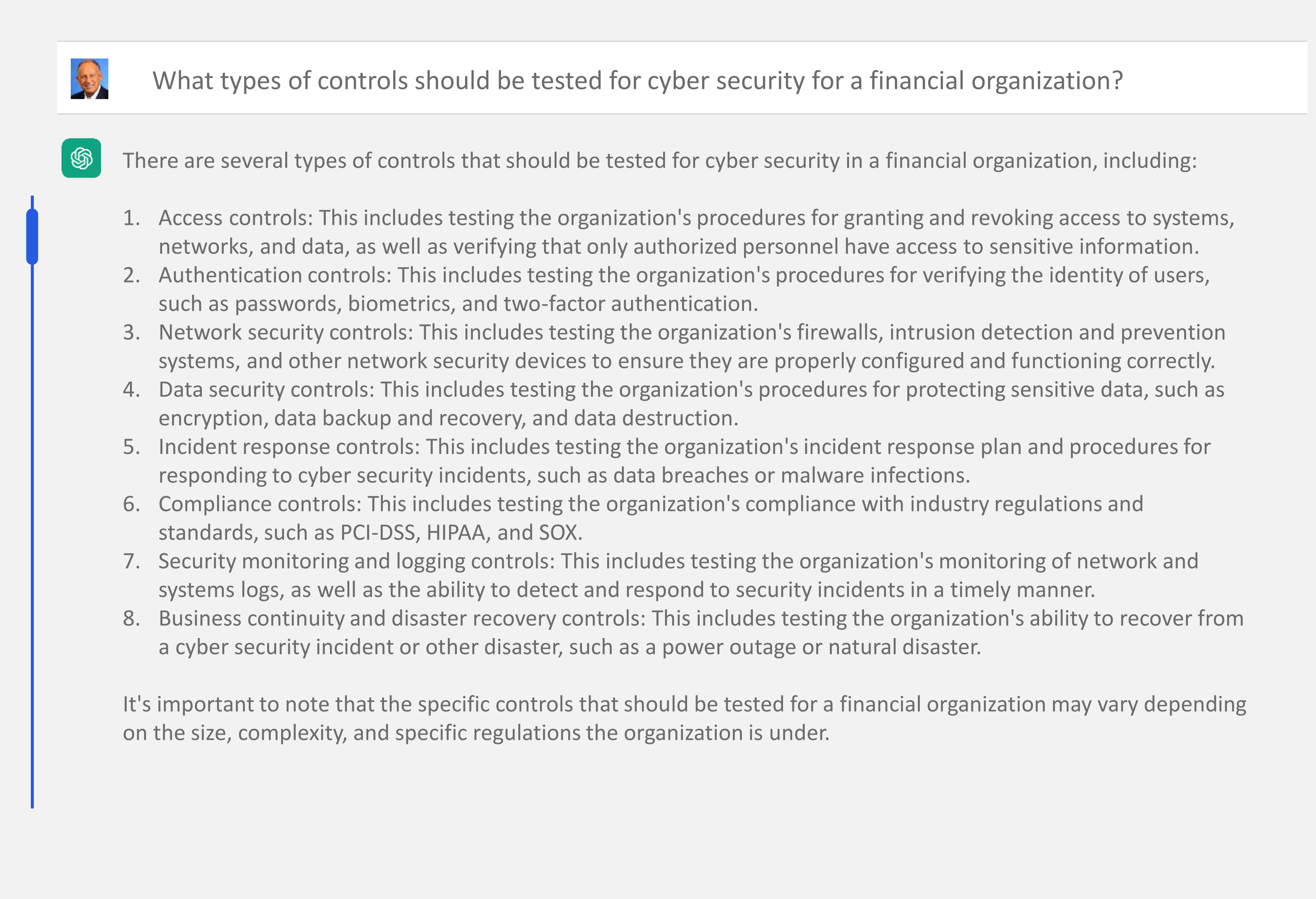
Big data allows us to bring billions of records of payment information under one single place to identify inconsistencies

BENEFITS

- Driving greater assurance
- Full population testing
- Identify thematics and expand root cause analysis

Exploring the Future

Large Language Models (LLM)



What types of controls should be tested for cyber security for a financial organization?

There are several types of controls that should be tested for cyber security in a financial organization, including:

1. Access controls: This includes testing the organization's procedures for granting and revoking access to systems, networks, and data, as well as verifying that only authorized personnel have access to sensitive information.
2. Authentication controls: This includes testing the organization's procedures for verifying the identity of users, such as passwords, biometrics, and two-factor authentication.
3. Network security controls: This includes testing the organization's firewalls, intrusion detection and prevention systems, and other network security devices to ensure they are properly configured and functioning correctly.
4. Data security controls: This includes testing the organization's procedures for protecting sensitive data, such as encryption, data backup and recovery, and data destruction.
5. Incident response controls: This includes testing the organization's incident response plan and procedures for responding to cyber security incidents, such as data breaches or malware infections.
6. Compliance controls: This includes testing the organization's compliance with industry regulations and standards, such as PCI-DSS, HIPAA, and SOX.
7. Security monitoring and logging controls: This includes testing the organization's monitoring of network and systems logs, as well as the ability to detect and respond to security incidents in a timely manner.
8. Business continuity and disaster recovery controls: This includes testing the organization's ability to recover from a cyber security incident or other disaster, such as a power outage or natural disaster.

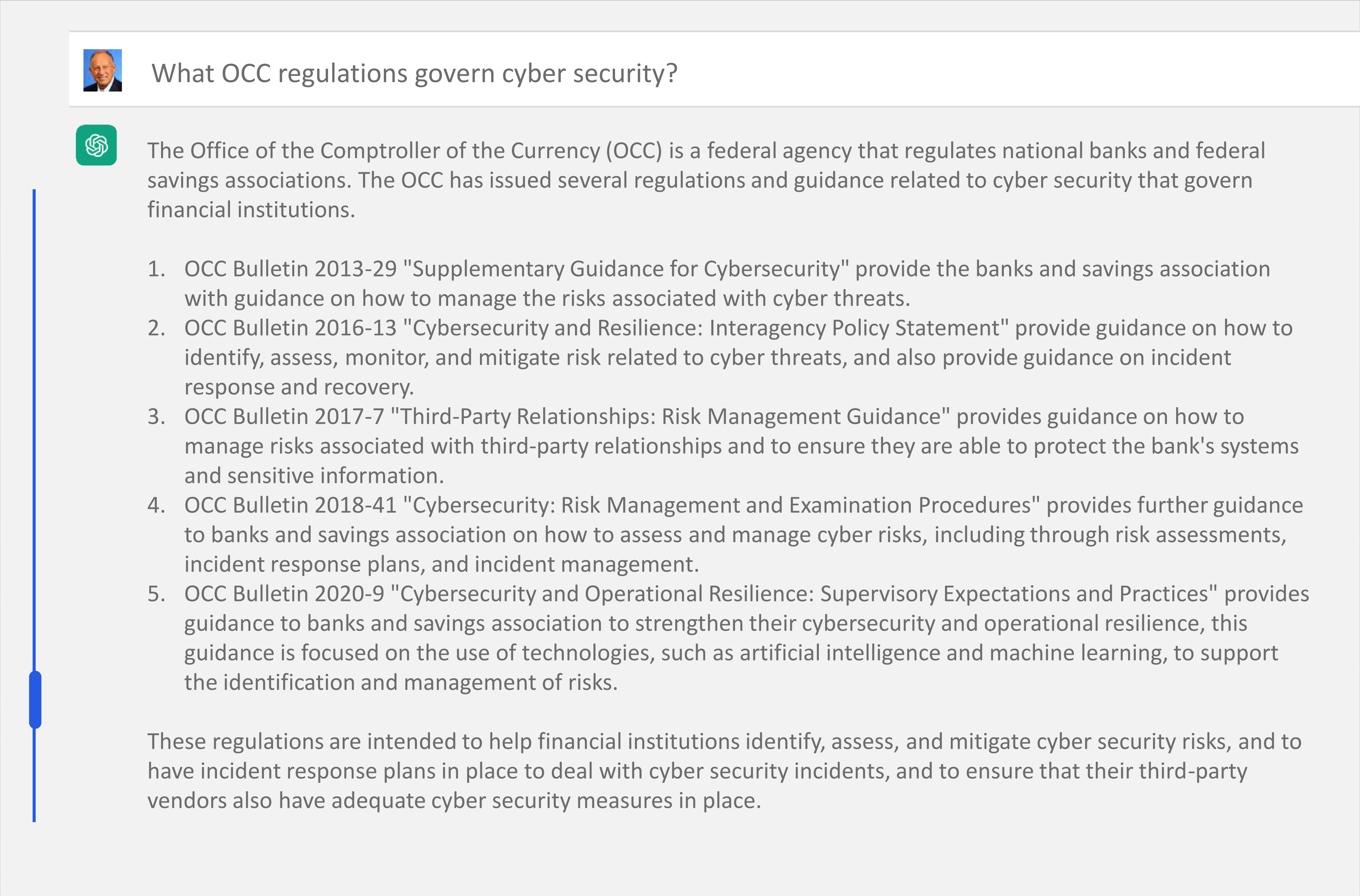
It's important to note that the specific controls that should be tested for a financial organization may vary depending on the size, complexity, and specific regulations the organization is under.

(POTENTIAL) BENEFITS

- Unlocks the power of cumulative knowledge
- Parsing insight usable and actionable format
- Improved customer service (e.g. dynamic chatbots, AI assistants)

Exploring the Future

Large Language Models (LLM)



What OCC regulations govern cyber security?

The Office of the Comptroller of the Currency (OCC) is a federal agency that regulates national banks and federal savings associations. The OCC has issued several regulations and guidance related to cyber security that govern financial institutions.

1. OCC Bulletin 2013-29 "Supplementary Guidance for Cybersecurity" provide the banks and savings association with guidance on how to manage the risks associated with cyber threats.
2. OCC Bulletin 2016-13 "Cybersecurity and Resilience: Interagency Policy Statement" provide guidance on how to identify, assess, monitor, and mitigate risk related to cyber threats, and also provide guidance on incident response and recovery.
3. OCC Bulletin 2017-7 "Third-Party Relationships: Risk Management Guidance" provides guidance on how to manage risks associated with third-party relationships and to ensure they are able to protect the bank's systems and sensitive information.
4. OCC Bulletin 2018-41 "Cybersecurity: Risk Management and Examination Procedures" provides further guidance to banks and savings association on how to assess and manage cyber risks, including through risk assessments, incident response plans, and incident management.
5. OCC Bulletin 2020-9 "Cybersecurity and Operational Resilience: Supervisory Expectations and Practices" provides guidance to banks and savings association to strengthen their cybersecurity and operational resilience, this guidance is focused on the use of technologies, such as artificial intelligence and machine learning, to support the identification and management of risks.

These regulations are intended to help financial institutions identify, assess, and mitigate cyber security risks, and to have incident response plans in place to deal with cyber security incidents, and to ensure that their third-party vendors also have adequate cyber security measures in place.

(POTENTIAL) BENEFITS

- Unlocks the power of cumulative knowledge
- Parsing insight usable and actionable format
- Improved customer service (e.g. dynamic chatbots, AI assistants)

Exploring the Future

The Metaverse

(POTENTIAL) BENEFITS

- Improves remote working challenges through virtual offices and meetings
- Interactive e-learning – ability to have a "hands-on" experience when learning new concepts

Learning and Development in the Metaverse

Virtual Onboarding

citi

Fostering a Culture of Innovation

For 2023, Internal Audit has launched the **Platinum Solution Recognition (PSR)** program, to highlight high impact, insightful solutions, with cross-functional and cross-regional applicability

IA’s **Future Ready Forum 2023** was a 2-day round-the-clock event covering a range of key topics such as advanced technologies, emerging risks, data quality, the latest industry trends and techniques to enhance our audits, and new audit tools to support the auditors of the future

We´ve also established the IA **Innovation Influencers Program**, bringing together an exclusive group of auditors who have demonstrated an ability to effect change, empowered to drive usage of innovative tools and techniques, further promoting an Innovative mindset