RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **RMG-F03**

Equifax Canada Multi-client Collaborative Cybersecurity Audit

Arif Hameed CISSP, CISA, CRISC

Senior Director, Client Security
Equifax Canada

Audit Odyssey — Working Towards the Same Outcome

TRANSPARENCY

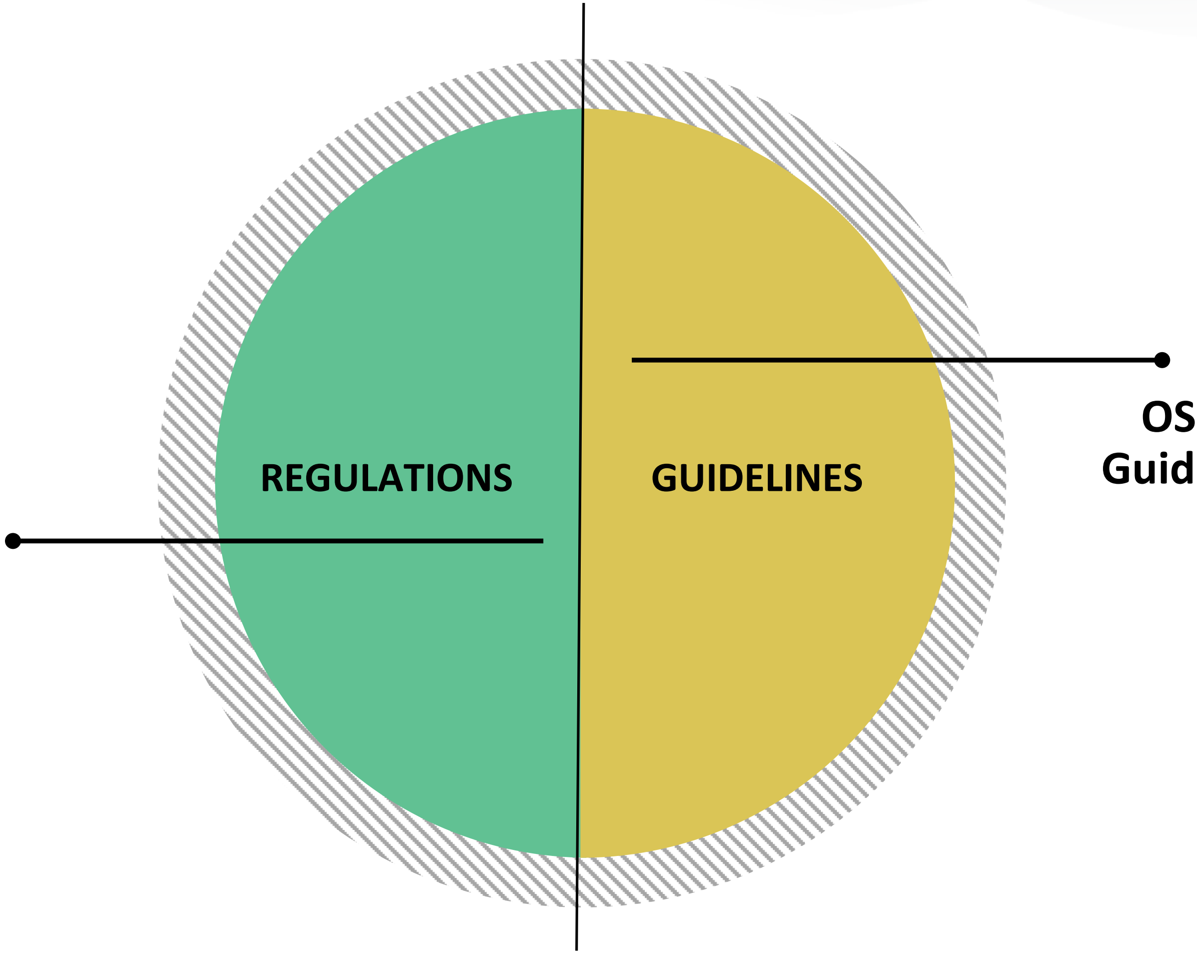
COLLABORATION

The landscape has changed, maybe more so now than ever

Why Go Above and Beyond?

Regulators & Vendor Due Diligence – The Details

With an **increase in regulations**, clients are conducting 3rd party due diligence



REGULATIONS

GUIDELINES

OCC 2013-29, OSFI B-10 and PRA Guidelines in UK and Australia

Current External Audits Are Not Enough

Security due diligence is quite stringent and industry standard reviews are often not seen as enough

Clients are looking for more granular testing of security controls around services relevant to them

REPORT	GAP
ISO 27001	Report is not shared and process oriented audit
PCI DSS RoC	Report not shared and limited to Cardholder Data Environment (CDE)
SOC SSAE18	Report does not have the depth needed

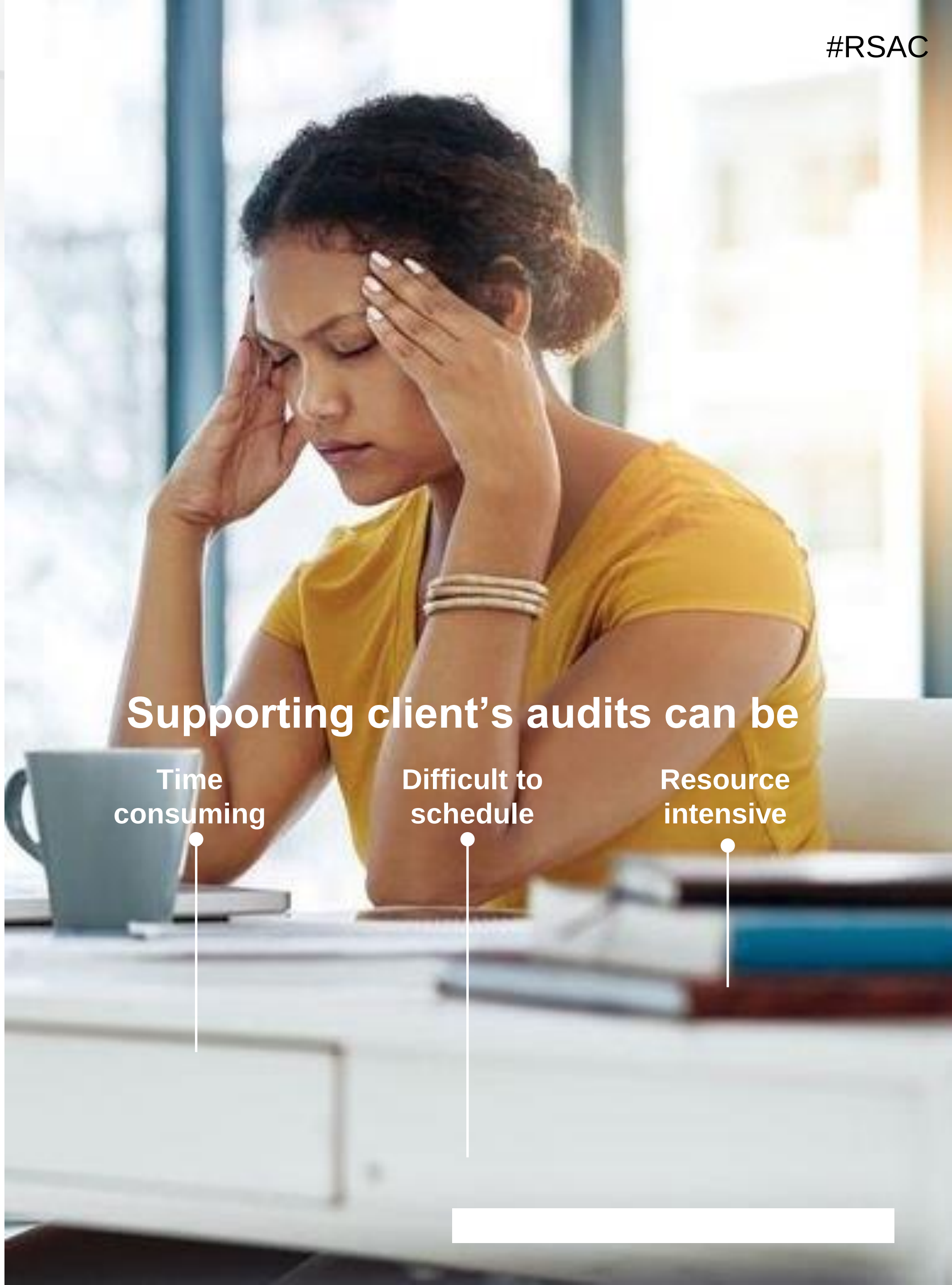
Managing Client Security Audits is Painful

Client On-site Cybersecurity Audits — Internal Challenges

1. Supporting client's audits is time consuming, difficult to schedule and resource intensive with InfoSec and IT teams under audit fatigue

2. Significant number of cybersecurity controls tested during client audits on EFX are similar across the clients as they normally align to industry frameworks such as ISO 27K1, PCI, NIST, CSA, ISF etc.

3. Remediation activities are at times duplicative and cumbersome to manage



Supporting client's audits can be

Why A Multi-Client Cybersecurity Audit Made Sense For Us

Equifax Canada as Testbed for New Initiatives

Equifax Canada is a smaller Business Unit (BU) than our US parent which makes it **an ideal environment to pilot projects that can be adopted** by other BUs of Equifax

Transformative culture at Equifax **encourages new concepts to boost efficiencies** where possible and even our biggest clients are open to collaboration with peers

OPTIONS FOR
COLLABORATIVE ASSESSMENT

Consortium

Consortiums have options to conduct on-site verification of security controls for their platform clients with external assessment firms

Major consortiums include TruSight, KY3P, CyberGRX etc.

Consortium solutions are still in their infancy, cost may be an issue to clients and their generic security assessments may not meet the scope of various clients. Client right to audit is still in effect and there is a risk of unauthorized disclosure of security audit reports.

OPTIONS FOR COLLABORATIVE ASSESSMENT

Custom Audit

Ideal solution for Equifax Canada is a security audit that is tailored to the client scope

Some of the internal business processes are complex and there are nuances specific to clients that a generic assessment would not cover; Equifax is not a vanilla service provider.

Most EFX clients in Canada are not using the Consortium reports.

- Yet the cost of annual audits for what in some cases is a significant number of 3rd parties for a client (including EFX) can be prohibitive, often leading to a risk based approach

How to Get Clients to Buy In

Approaching Clients to Participate

Gaining buy-in from the Client's Cybersecurity team is critical; if they are not supportive this is a non-starter

1. **Arranged meeting with Head of Information Security** or their delegate that oversees supplier cyber risk; failure to engage correct stakeholder led to delays in client participation

2. **Engaged client's stakeholders** such as Procurement, Vendor Management, Risk Management and LoB Relationship Owners; at minimum they need to be aware as they could raise obstacles around buy-in

Overcoming Hurdles

1

Clients were from a range of industries and their supplier risk approach differed greatly

We only approached large FIs and Telco customers, as similar services made scoping easier and they were more receptive to the concept

2

Assurance around the assessment was a concern

To allay this concern, we notified clients that we would engage an independent reputable 3rd party assessment firm at our expense to perform the assessment

3

Timeline to complete

We ensured that the final report would be released to clients by October 31 at the latest to align with year end banking client's reporting deadline

Overcoming Hurdles

4

Some of the original participants retired leading to new discussions after the work was already done – more than one!

5

Some Legal teams joined the discussion after the fact and made discussions extremely challenging….they were looking for the trick we were playing

Scoping the Controls and Selecting the Right Partner to Deliver Results

SIG as the Baseline for Audit Scope

Scope Selection Delivery

Clients from the FIs **and** Telco are sending industry standard as well as customized questionnaires with the most common one being the Shared Assessments SIG over those based on ISO27K1 or NIST CSF

- Latest version of the SIG was mapped to the participating clients questionnaires; this was a very time consuming manual task as there were a number of controls that were loosely mapped
- Deltas were also identified and many were noted in Physical Security and Risk Assessment domain areas

Key Control Selection

Scope **Selection** Delivery

IDENTIFICATION OF CONTROLS

There were over 1,000 controls identified amongst the client questionnaires and the SIG

DEFINING OF SCOPE

The scope was limited to Cybersecurity; Privacy and Compliance domains were removed and Cloud Security was not in scope

SEND-OFF, APPROVAL AND FEEDBACK

A subset of key controls across the domains with a focus on IAM, Network Security, AppSec, and Crypto were selected and sent off to the clients for their feedback and approval

SELECTIONS AND TESTING

Total of ~350 agreed upon controls were selected for testing

Assessment Firm Selection

Scope **Selection** Delivery

CONFLICTS OF INTEREST

To avoid a conflict of interest, Big 4 firms were not in consideration as both Equifax and respective clients had audit and/or consulting relationships in place

SECURITY AND CONSULTING FIRMS

We looked at other nationally recognized accounting and security consulting firms

TOP 10 ACCOUNTING FIRMS

We chose a US top 10 accounting firm that had a strong third party cyber risk practice with experience performing vendor cybersecurity assessments for banking clients

CHOOSING YOUR FIRM

Depending on the nature of your business, a Security Consulting firm may make more sense instead of an accounting firm

Report Format

Scope Selection **Delivery**

EVIDENCE BASED APPROACH

Evidence based approach was followed, hence operating effectiveness testing was performed

TESTING MATRIX

Testing matrix was included in the report that detailed the testing procedure, outlined explicit details on the operational evidence reviewed and the result of the test if there was an observation

FINDINGS AND SEVERITY

As each client has their own risk methodology, it was at their imperative to determine whether an observation was a finding and at what severity

CONSISTENT REPORT

The report was consistent for all clients for the most part; the only nuance would be an additional business service that may not be relevant to other clients

Audit Execution

Scope Selection **Delivery**

AGREEMENTS

Control procedures were agreed upon with the audit firm but were primarily based on the SIG Shared Control Assessment (SCA) procedures

PRE-AUDIT MEETINGS

To save on fees, the internal InfoSec team conducted pre-audit meetings to identify controls, collect evidence and handle logistics with SMEs

DATE SELECTION

The date was selected to avoid scheduling conflicts with annual ISO 27001, SOC and PCI DSS audits

ON-SITE AUDIT

The audit was conducted on-site at US HQ for the Enterprise managed controls and in Canada for the Equifax Canada managed controls

Audit Benefits

BENEFITS of the Audit to Clients

Saved costs, time, and resources

Provided independent assurance by a top accounting firm

Closed the “audit gap” across firms

Shared questions across clients. More comprehensive than independent audits

BENEFITS

# of the Audit to Equifax

Saved the team ~500 work hours

Enabled **streamlined prioritization** of audit observations

Created a **collection of evidence** for common controls used for both the multi-client audit and other audits

Tips to Make it Easier

APPLY

Implementing a Collaborative Cybersecurity Audit

Identify clients with similar audit requirements

- Same or similar industries
- Share control requirements
- Audit in-depth

Develop a common controls set

Select an assessment firm that has expertise on third party cyber risk

RSA Conference2020

Questions