NAVEX™

Fireside Chat – 3 IRM Trends & Predictions for 2022

- Kyle Martin, Senior Director, Customer Success & Professional Services, NAVEX

  Matt Crome, Senior Manager, Customer Success & Partner Services, NAVEX

Agenda

- Implementing a Privacy Framework
- Addressing IT Risk to Build Business Resiliency
- Developing a Third-Party Risk Management Program
- Conclusion

Presenters

Matt Crome

Sr. Manager, Customer Success & Partner Services

NAVEX

Kyle Martin

Sr. Director, Customer Success & Professional Services

NAVEX

Implementing a Privacy Framework

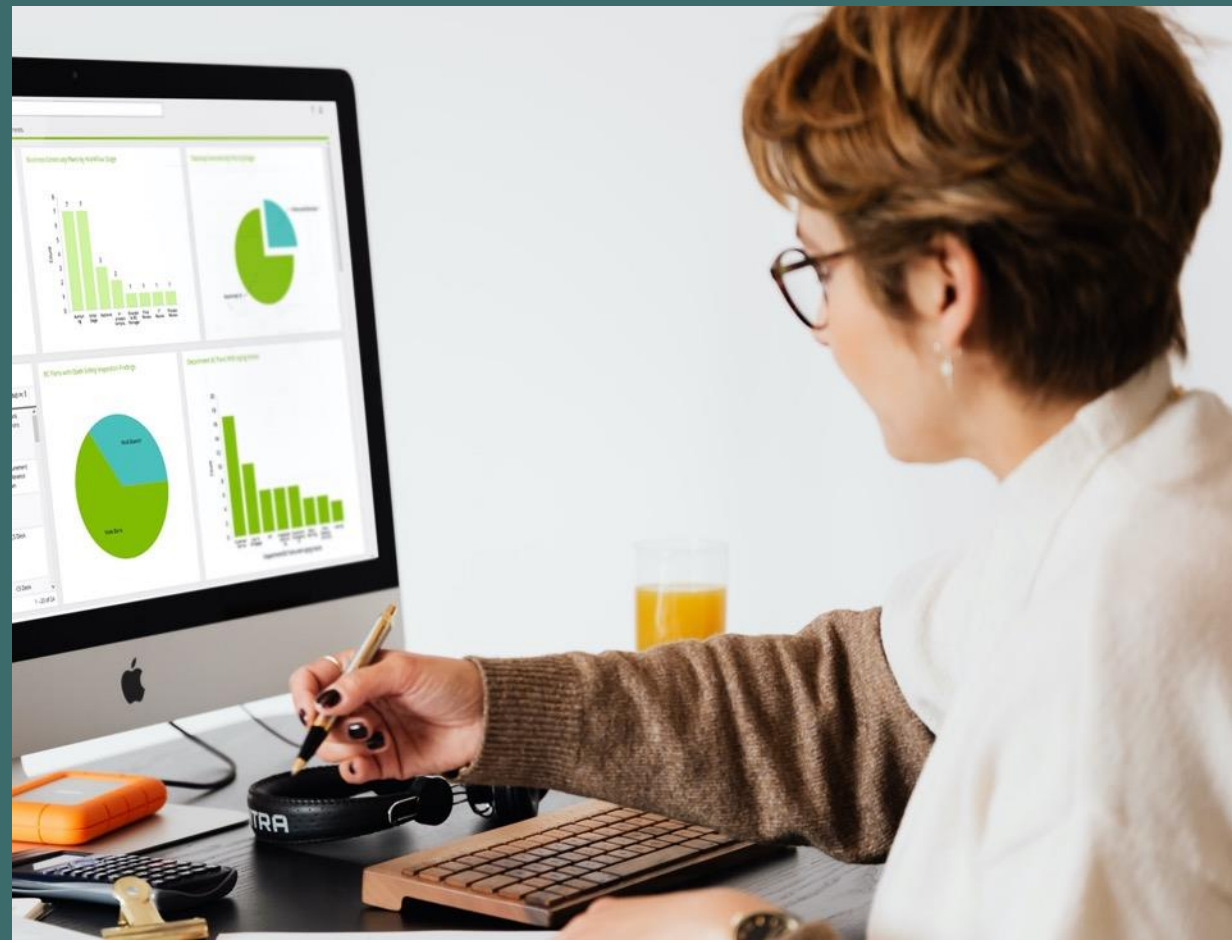
Poll Question

How mature is your company's data privacy program?

- No program in place currently
- Siloed programs, independent/ad hoc management
- Definitive privacy model but very reactive
- Fully integrated and proactive privacy solution

Expanding Requirements

- Choosing the right framework
  - Is there a clear grasp of requirements?
  - Does it apply to the business?
- Appetite for risk
  - Focusing on productivity
  - Natural frustration with compliance
- Framework examples
  - Fair Information Practice Principles
  - ISO27701
  - National Institute of Standards and Technology (NIST) Privacy Framework

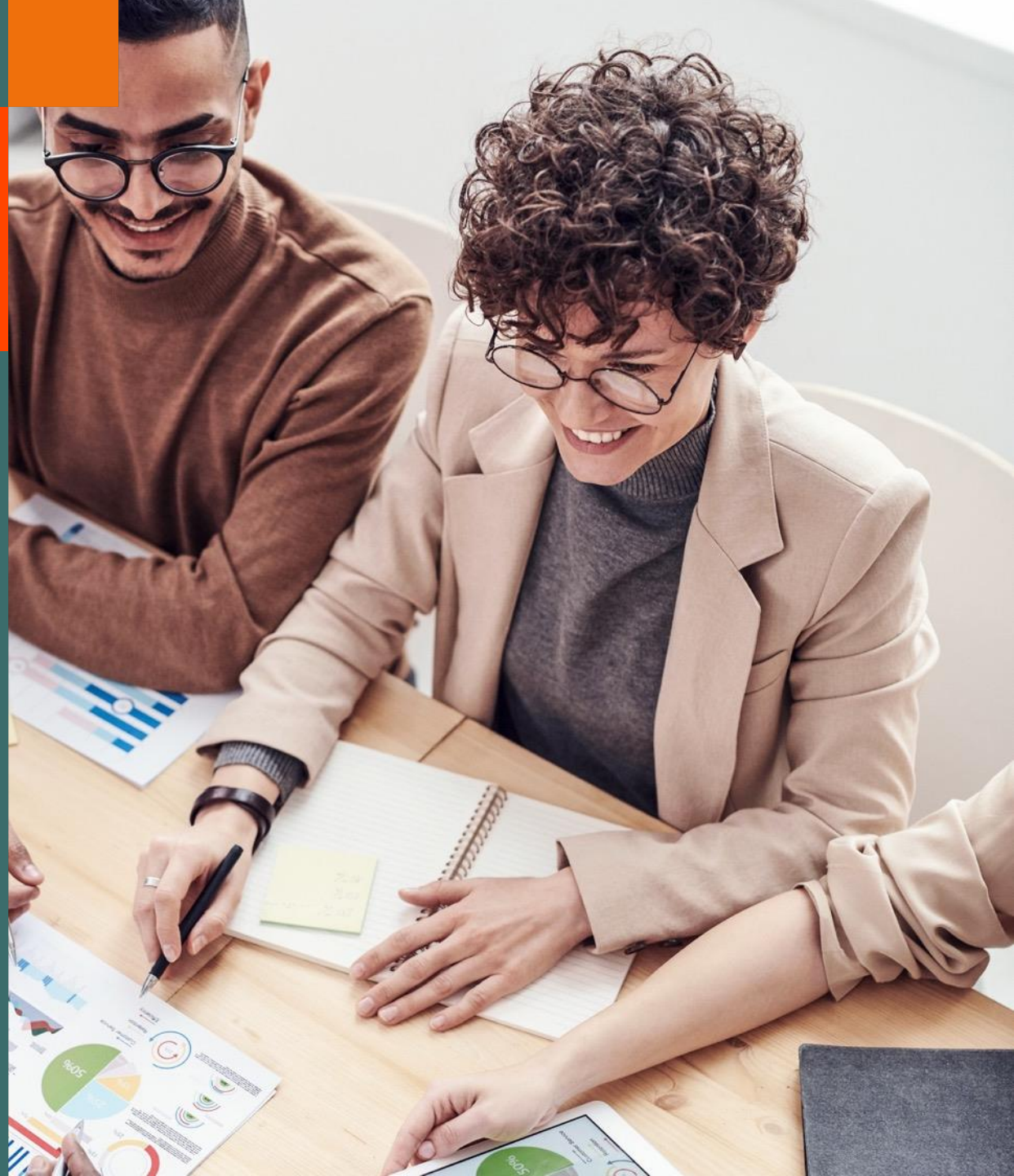


NAVEX™

Buy-in

- Starts with Executive Management
- Is there a Steering Committee?
- Harmonization of controls – test once, satisfy many
- Where can we leverage our existing policies, procedures, and training
- The shift to technology
  - Advantages of automation in preparation and response
  - Ability to report incidents quickly
  - Dynamic models
  - Bridging the gap to IT Risk Management

Addressing IT Risk to Build Business Resiliency



Poll Question

How supportive or integrated are your IT Risk and Business Continuity teams and processes?

- Completely Independent
- Related in scope but no shared systems
- Some data exchanged (one direction)
- Highly integrated (data and processes exchanged regularly)

Consider the Basics

- Align core functions of IT with core functions of BC
  - Back-ups & Recovery
  - Physical/Network Security
  - Maintenance
- IT, Technology, & Risk Management's role
  - Facilitator – Assessments & Planning
  - Solution – Work-Arounds, back-ups
  - Instigator – Source of problems
- Don't rely on reactive tools without proactive planning (or vice versa)

Know the Problems (and the Solutions)

"Traditional" Threats

- Software issues & Malware
- Cyberattacks or Data breaches
- Physical infrastructure loss and natural disasters
- Failure and interruption of connections

New Focuses/Influences

- ESG
- Hybrid & Remote Work
- Rapid regulation growth & change

People

- Part of the problem, and a bigger role in the solution

Integration, automation, communication

- Address the basics of patching
- Utilize analytics/data AND team feedback
- Ensure information is securely housed but reportable collectively

Bend (and sometimes break)

- Adapt process and procedure, but be comfortable (and prepared) to change or start something new

NAVEX™

Developing a Third-Party Risk Management Program

Poll Question

How critical does your organization consider a holistic approach to TPRM?

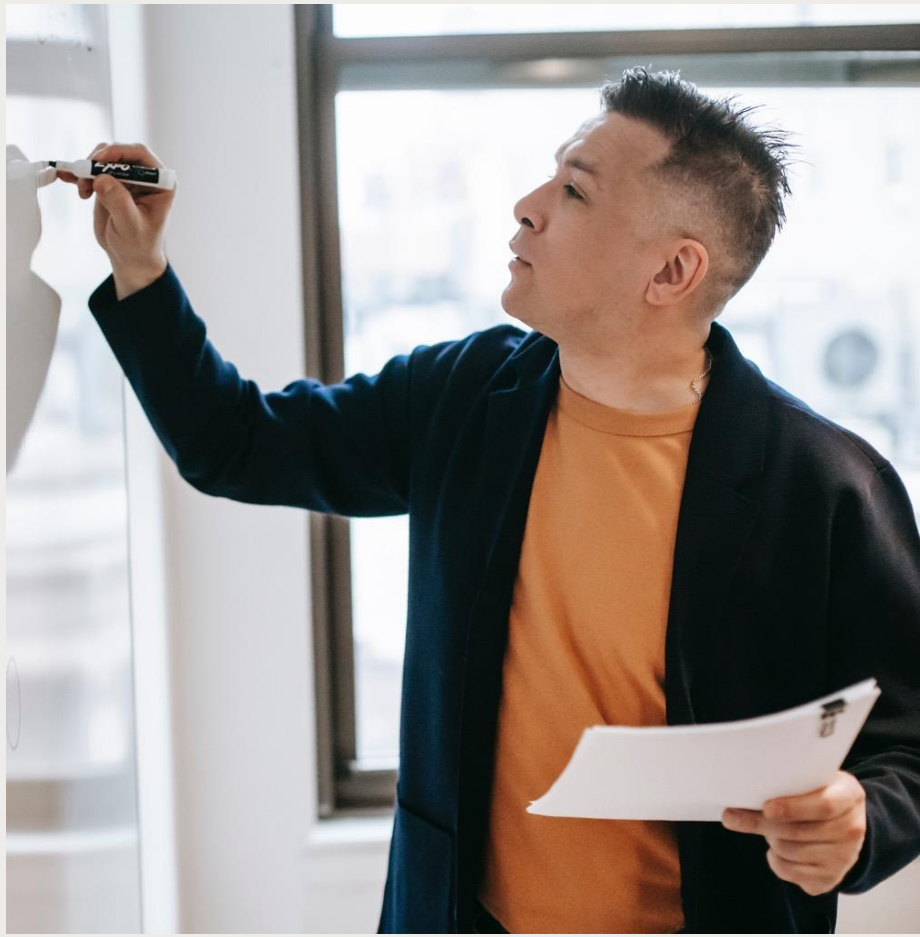
- No program in place / TPRM is independent
- Low priority / TPRM is a step in another team's process
- High priority
- Absolutely critical

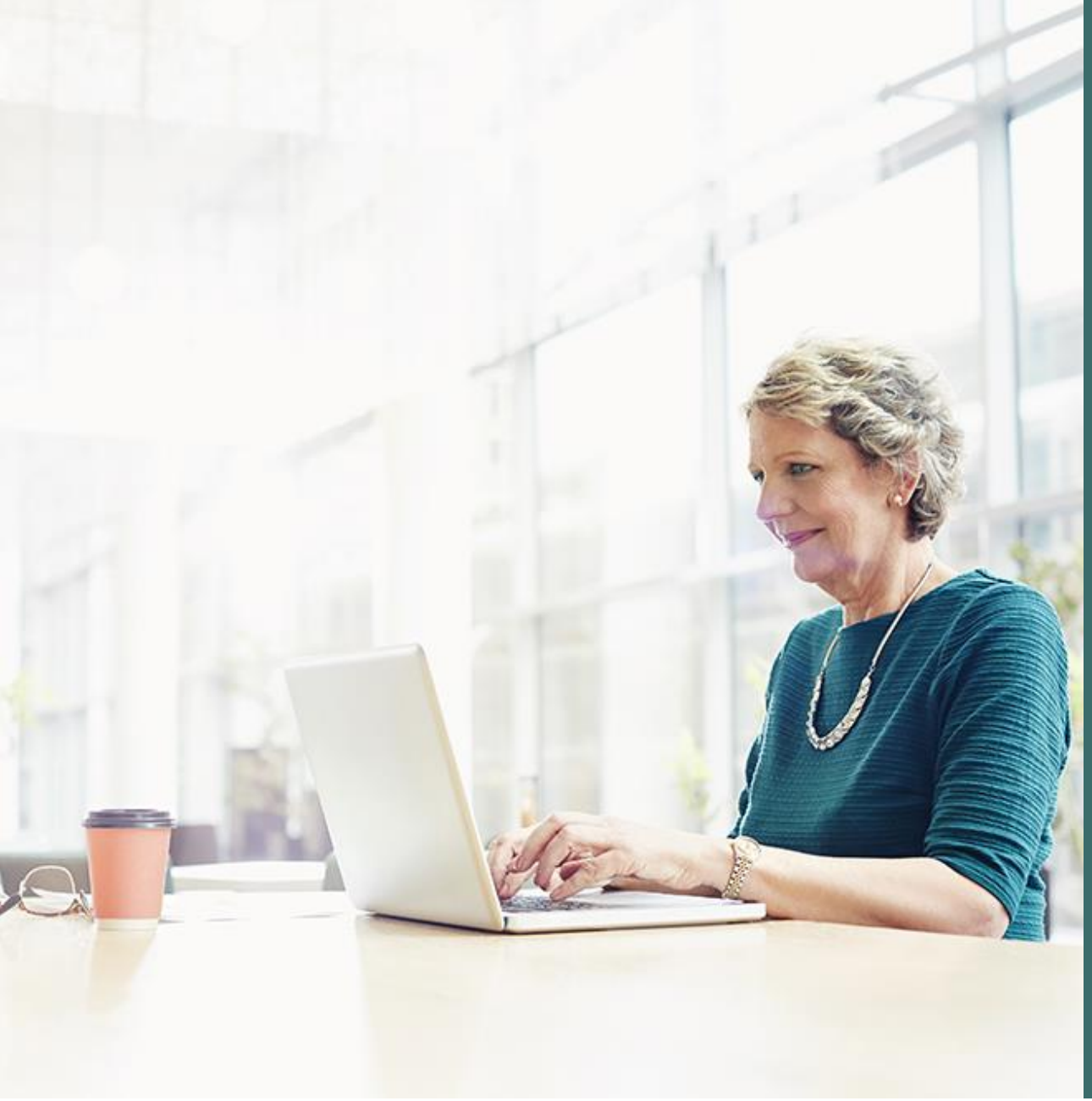
Quality Over Quantity

- Make your assessment and monitoring process work for third parties, not against you. Better relationships equal better information. Hold them accountable, but don't make it frustrating to do business with your organization.

- Focus on core questions and key results. You probably don't need to ask that many questions.

- Monitor continuously and reactively. Reassess your third parties based on criticality and incorporate SLA tracking into your technology. Be ready and able to collect "ad hoc" responses (Log4j, Treasury sanctions).





Be Proactive and Intentional

- Create controls BEFORE regulations catch up and start incorporating them into your assessments.
- Tie your questions to those controls.
- Establish a Vendor Risk Profile for your initial decision and ongoing monitoring.
- Understand how to incorporate fourth party compliance.
- What is your organization's compliance commitment?

NAVEX™

Thank you.

NAVEX™

