October 25, 2024

Help! I am Being Audited

Navigating Cybersecurity & Data Privacy Program Assessments

Aveen Sufi
Dexcom

Mac McCullough
Troutman Pepper

Ryan Smyth
FTI Consulting

Privacy+ Security Forum

Speakers

Privacy+ Security Forum

Mac McCullough

Senior Privacy & Security Advisor

Troutman Pepper

Aveen Sufi

Sr. Manager Global Privacy & AI Governance Chair

Dexcom

Ryan Smyth

Managing Director

FTI Technology

- Welcome and Introductions
- **Part I – Understanding Audits** (What)
  - Audit Types & Key Things to Know for Each
  - Getting Audit Ready
  - What to Expect
- **Part 2 – Leading Through Audit** (How)
  - Framing
  - Preparing
  - Managing
  - Post Audit Priorities
- **I'm Being Audited Top 10**
- Q & A

Part I

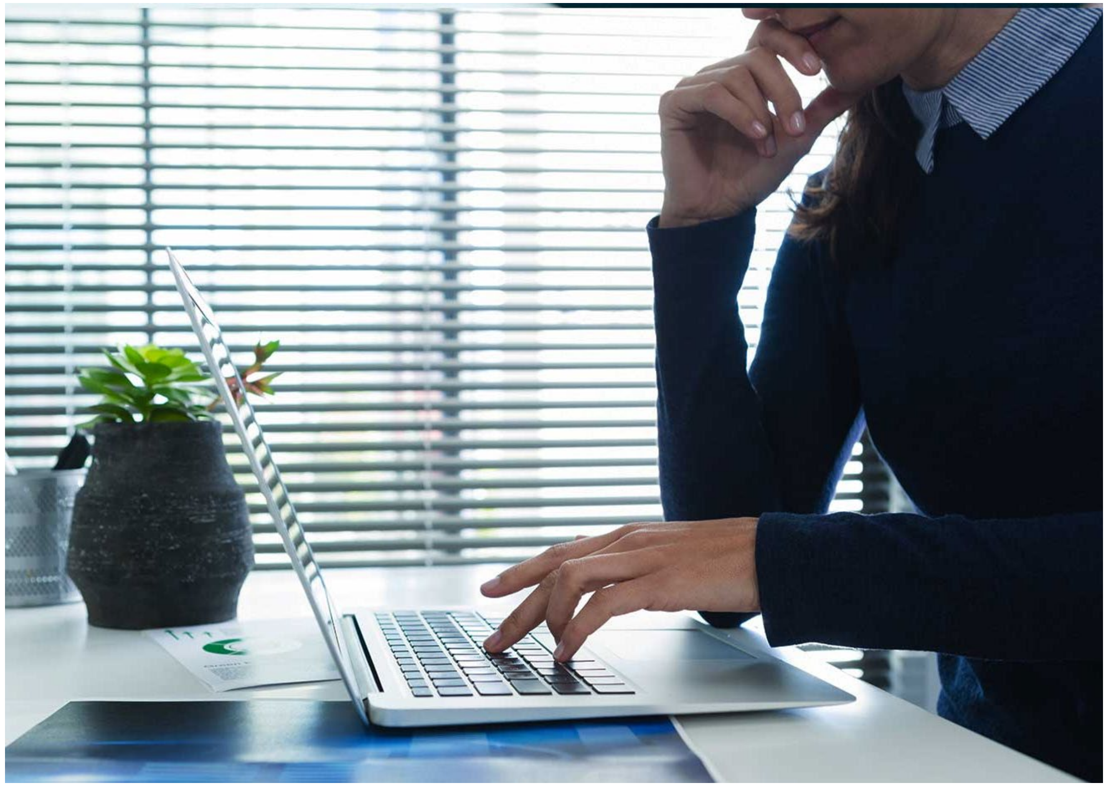
Understanding Audits

Audit Types & Key Things to Know for Each

Audit Types & Key Things to Know for Each

Privacy+ Security Forum

- Internal Audits
- Regulator Audits
- 3rd Party Assessments
- SOC Reports, ISO Certifications, PCI, etc.



Part I

Understanding Audits

Getting Audit Ready

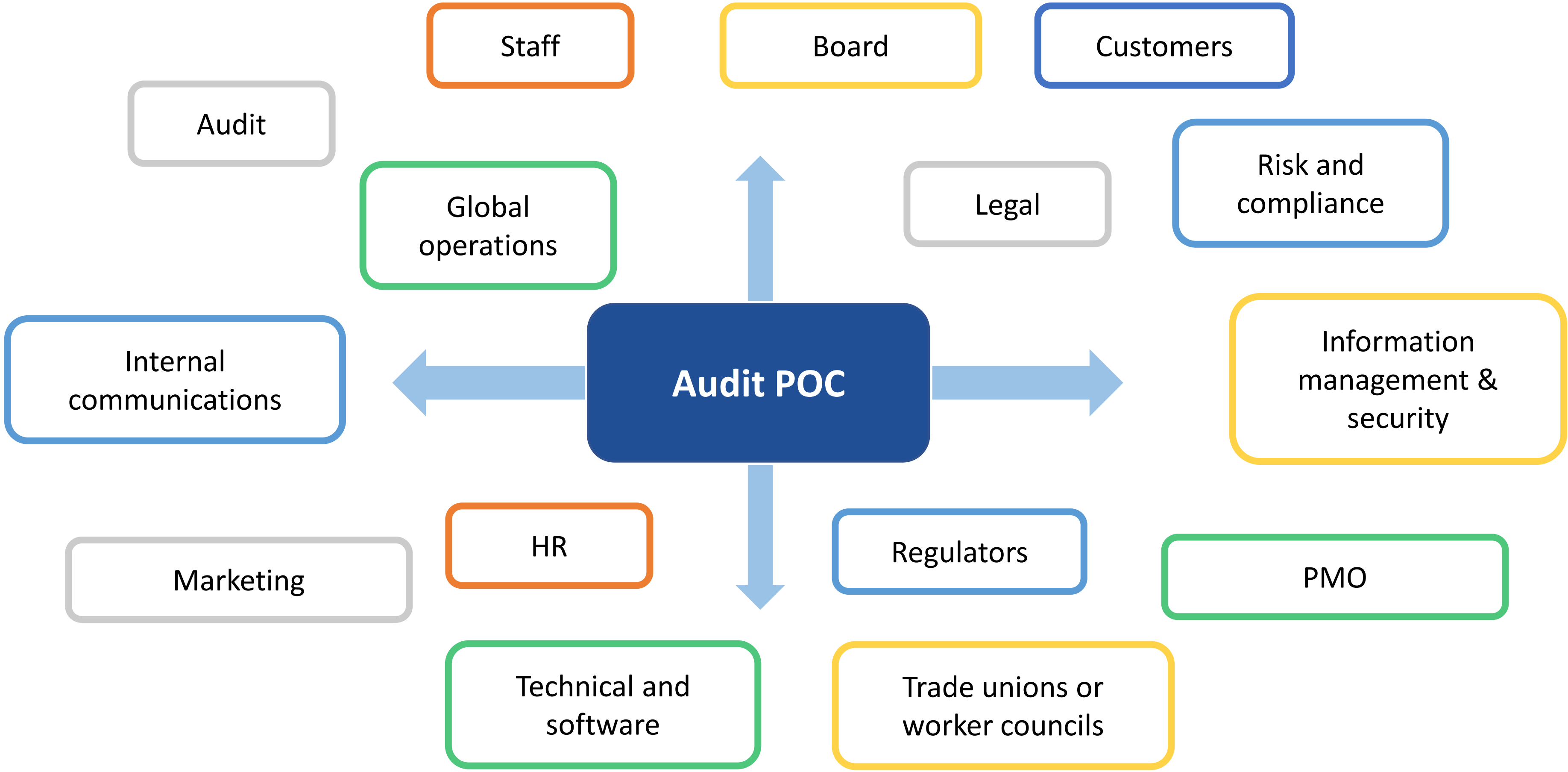
Privacy+ Security Forum

Getting Audit Ready

- **Pre-work and being ready**
- **How is your privacy function defined?**
- **Are roles and responsibilities defined?**
- **Are your privacy operations “auditable”?**
- **Do written policies reflect reality?**
- **Who will be the primary POC/point person?**

Managing Stakeholders and Sponsors

Privacy+ Security Forum



Audit Logistics

- What information can be shared externally?
- Secure document portal
- Facilitate timely access to SMEs and other Stakeholders
- Review and Redact Samples and Documentation

Part I

Understanding Audits

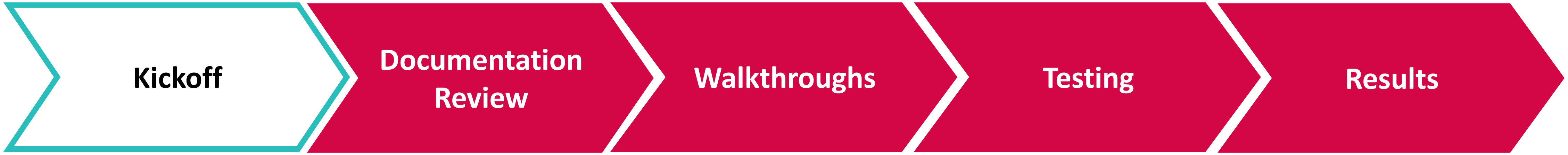
What to Expect

What to Expect

- Initial Kick-off and Scoping Meeting
- Document Request Process
- Control/Process Walkthroughs
- Testing and Effectiveness Assessment

Kick-Off, Planning and Scoping Workshop

- Introduce project, objectives, approach, methodology, etc.
- Socialize timeline with key stakeholders
- Agree on project assumptions
- Confirm programmatic, substantive, and geographic scope
- Discuss work steps, level of effort, division of labor
- Agree on terminology to be used throughout engagement
- Determine communication protocols, status reports, and other logistical items essential for project success
- Define desired outcomes and project deliverables



Kickoff

Documentation Review

Walkthroughs

Testing

Results

Document Request Items

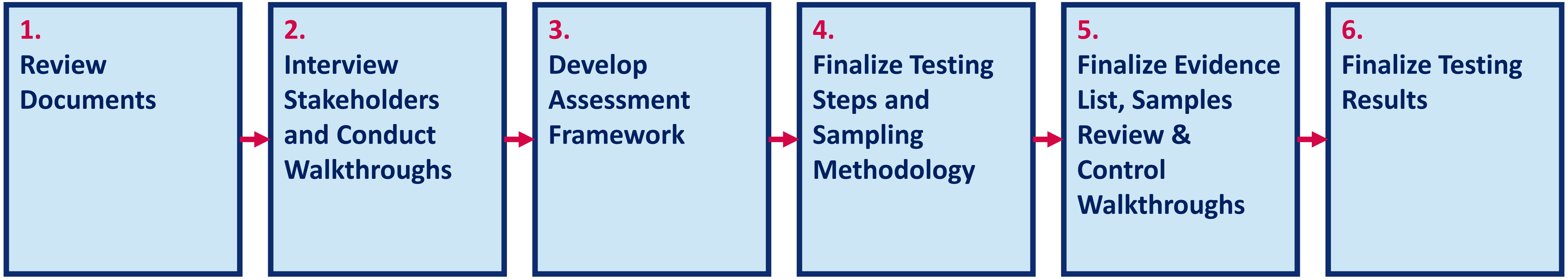
- Privacy Function Organizational Charts
- Internal and External Privacy Policies and Notices
- Summary of Prior Assessments
- Information Security Policy
- SDLC/Change Management Policy
- Record Retention and Deletion Policy
- Roadmaps
- Past or Current Open Issues
- Process Maps
- Control Environment Documentation

Control Testing Methodology

- **Document Review:** Conducting a review of policies, procedures and supporting evidence to validate Client’s privacy program and related controls.
- **Stakeholder Interviews:** Interviewing Client stakeholders to better understand privacy controls and validate control activities.
- **Observation:** Walkthroughs of Client’s privacy controls to assess the design of the controls. This could include demonstrations of tools or systems used to perform a privacy control or to review documents subject to confidentiality restrictions.
- **Sampling and Testing:** Selecting and reviewing data from Client’s operations during the reporting period to validate the effectiveness of Client’s privacy controls. This could include sampling of training records, change management tickets and privacy impact assessment results.

Independent Assessment Methodology

- Order requirements
- Management assertions and control statements for the reporting period
- Applicable privacy regulations and standards
- Risk level associated with each control



1. Review Documents

2. Interview Stakeholders and Conduct Walkthroughs

3. Develop Assessment Framework

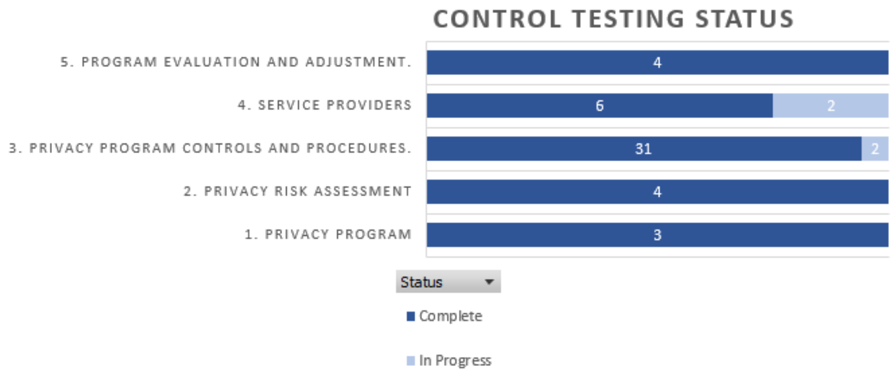
4. Finalize Testing Steps and Sampling Methodology

5. Finalize Evidence List, Samples Review & Control Walkthroughs

6. Finalize Testing Results

Project Planning and Status Reporting

Control Group	Total Controls	Docs Requested	Docs Received	Populations Requested	Populations Received	Samples Requested	Samples Received
1. Privacy Policy	3	3	3	0	0	0	0
2. Risk Assessment	4	4	4	0	0	0	0
3. Procedures	33	15	14	19	19	19	19
4 Third Party Risk Management	8	5	4	4	4	4	4
5. Training and Awareness	4	1	0	2	2	2	2


CONTROL TESTING STATUS

Overall Status		Budget	Scope	Schedule	Resource
	On Track	On Track	On Track	Off Track	On Track

Activities	Status	Start Date	End Date
Phase 1: Project Initiation		**2/1/22**	**2/15/22**
Kick off Meeting	Complete	2/1/22	2/1/22
Information Gathering / Schedule Stakeholder Interviews	Complete	1/26/22	2/11/22
Phase 2: Program Review and Control Mapping		2/8/22	3/1/22
Review Management Assertions/Privacy Controls	Complete	2/8/22	3/1/22
Develop Testing Steps and Sampling Methodology	Complete	2/8/22	3/1/22
Conduct Stakeholder Workshops	Complete	2/17/22	3/8/22
Phase 3: Control Testing		**3/1/22**	**4/30/22**
Confirm Sampling Testing Methodology	Complete	3/1/22	3/12/22
Conduct Sampling and Testing	Complete	3/4/22	4/16/22
Document Test Results	Complete	3/8/22	4/16/22
Present Preliminary Observations to Client	On Track	4/29/22	4/29/22
Finalize Testing Results	On Track	4/21/22	4/30/22
Phase 4: Reporting		**4/30/22**	**5/14/22**
Conduct Any Required Follow-Up	On Track	4/30/22	4/30/22
Draft Assessment Report	On Track	4/30/22	5/5/22
Present Draft Report to Client		5/5/22	5/5/22
Incorporate Client Feedback		5/5/22	5/7/22
Conduct Quality Control		5/10/22	5/13/22
Deliver Final Report		5/14/22	5/14/22

Part I

Understanding Audits

Post-Audit Priorities

Post-Audit Priorities

- **Retrospective**
- **Management Action Plans**
- **Remediation Activities**

Part II

Leading Through Audit

Framing

Privacy+
Security
Forum

Framing the Audit

- **What Game You Playing?**
  - There’s a difference between Audit and Assessment

- **Authority/Limit of Authority (Scope)**
  - What authority does Audit/Assessor have to conduct audit?
  - What are the limits of that authority?
  - How do those limits affect SCOPE (included/excluded from review)?
    - Negotiate scope ahead of time

- **Who is Performing the Review?** (See also Preparing: Choice of Reviewer)
    - State Regulator, OCR, PCI Counsel (PFI), Law Firm, Accountancy, Consultancy

- **What is the Duration of the Review?**
  - What are the start/stop dates?
    - Reviews should be specific in scope and TIME

Part II

Leading Through Audit

Preparing

Preparing

- **What is the Frequency of Review ?**
  - Is the review 1 time, annual, biennial or some other periodicity?
    - <u>Review frequency effects:</u>
      Goal setting and attainment; preparation planning; budgeting; timing of review (during or right after breach; major corporate event)
- **What Are Your Goals**
  - Prefer small, short term IO’s or more strategic IO’s?
    - Consider the frequency of review and potential impacts of review
    - Consider your budget and staffing
  - There will always be IO’s (see also Managing: Relationship Building)
    - Guide assessors to IO’s that are consistent with goals
    - Guide findings to allow organization to show continual improvement
- **Choice of Reviewer**
  - Often get to select reviewer
    - Examine credentials (CGEIT vs CISM vs CISSP/IAPP Fellow vs CIPP)
    - Do they have people that look like you? (Industry/In-house)
    - Is appropriate team on offer?

BY FAILING TO PREPARE, YOU ARE PREPARING TO FAIL.

BENJAMIN FRANKLIN

Part II

Leading Through Audit

Managing

Privacy+
Security
Forum

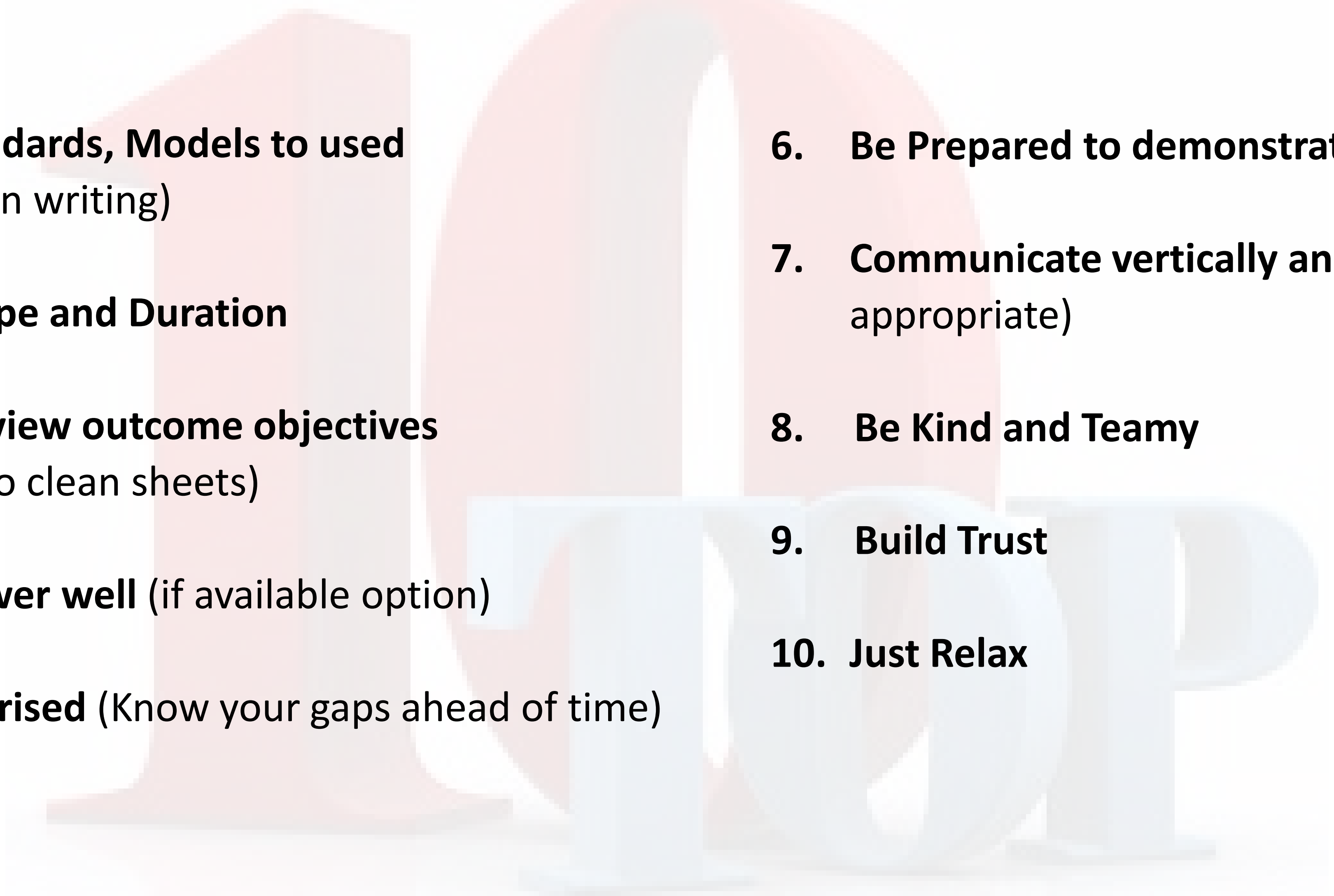
Managing

- **Build relationship with your reviewers**
- **Build trust with your reviewers**
  - Do what you, say what you do
  - DO NOT LIE. If you are going to mislead, do so at your own peril (almost never worth it)
- **Demonstrate preparedness**
  - To the extent advantageous or manage cadence
- **Manage Action Plan & Timing**
  - Required or Recommended? Risk-Based?
  - Be clear about dependencies. Fit roadmap?
- **What if you find something bad?** (Either in Prep or Manage Phases)
  - What actions should be offered/taken to ameliorate?
    - HR escalations? 3rd Party reassessment; contract amendment?
    - Blackout period

Top 10

Privacy+ Security Forum

Help! I'm being audited Top 10



1. **Negotiate Standards, Models to used** (require them in writing)

2. **Negotiate Scope and Duration**

3. **Know your review outcome objectives** (Remember, no clean sheets)

4. **Choose reviewer well** (if available option)

5. **Don't be Surprised** (Know your gaps ahead of time)

6. **Be Prepared to demonstrate**

7. **Communicate vertically and horizontally** (as appropriate)

8. **Be Kind and Teamy**

9. **Build Trust**

10. **Just Relax**

Questions?

Questions & Contacts

Mac McCullough

Senior Privacy & Security Advisor

Troutman Pepper

+1 (312) 759 3650
mac.mccullough@troutman.com

Aveen Sufi

Sr. Manager Global Privacy & AI Governance Chair

Dexcom

+1 (317) 430 7848
aveen.sufi@dexcom.com

Ryan Smyth

Managing Director

FTI Consulting

+1 (619) 572 3074
ryan.smyth@fticonsulting.com