**CHEAT SHEET** 



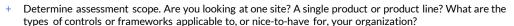
# **Security Assessment**

Consider these insights when planning or conducting an assessment or audit.

# **SCOPING CONSIDERATIONS**

### **Before You Start**

- + Have something in place: some written policies, some technology, a way to measure your controls.
- + Set expectations internally. What are your goals? Luring investors, targeting clients, expansion, a merger or acquisition?







### **Organizational Obligations**

- + Identify relevant locations, such as headquarters, where you generally operate, and/or where clients are located.
- + Determine which industries you will measure for.
- + Consider your organization's future plans and state (expansion, mergers and acquisitions).
- Determine your customer compliance requirements, whether through contractual obligations, or your market's wants and needs.
- + Make sure sales and security align with customer expectations and requirements.
- + Identify any other legal or regulatory compliance requirements.
- + Understand the overlap between security and privacy. Decide whether privacy makes sense for the organization in relation to costs and time.

#### **Technology Considerations**

- Determine how your data is housed and how data centers are being managed: cloud, on premises, locations within the scope.
- + Articulate what security tools you have.
- + Identify products and assets, such as applications and devices used.



#### **Scoping Output**

- + Decide what level of complexity you seek in reporting. A deep dive into every control can yield hundreds of pages, while a more limited scope results in lighter reporting.
- + Consider how much time you will have.
- Identify available resources.



# TEAM AND ARTIFACT PREPARATION

#### **Knowledge Consolidation and Storage**

+ The up-front availability of policy and process documents is the best way to prevent delays later in the process. Have documentation and information ready for: baseline configurations, network diagrams, security technology map, and anything else that will consume assessment or audit time if built or discovered after the preparation phase.



#### **Communication Expectations**

- + Compensate for delays due to a remote workforce.
- + Decide who will answer for all the different domains involved.
- In terms of project management, decide who will drive it. Will there be coordination with a vendor's project management team?
- + Maintain open disclosure and honesty in your own preparation process and self-assessments.
- + Response time is important, leverage momentum as memories are fresh and focus is sharp.



# **Time Considerations**

+ You are assessing a point in time, so be clear about that time period and what is relevant.



# REMEDIATION

### **Time Commitments**

- + Are you building a 3-year roadmap or 1-year list of projects?
- + Identify any completion deadlines and sales commitments or contractual obligations. It is crucial to plan back from those dates or push back early on.
- + Consider budget timing. Do you have a model for CapEx vs OpEx? Will you outsource or hire internally?



#### **Remediation Impacts**

- + Identify investor expectations.
- + Ensure that actions support client contracts.
- + Understand technology and implementation costs for deployment of new policies.



#### **Rinse and Repeat**

- + Ultimately, an audit format will closely resemble an assessment format.
- + Leverage the yearly recurrence of most assessments and audits and develop a preparation routine.
- + With constantly changing controls, focus on developing repeatable assessment processes.

