Example: CISO's Presentation Script: Board Workshop on Risk Appetite

This document provides a slide-by-slide script for the CISO to facilitate the board workshop on defining the organization's risk appetite and tolerance.

Associated Documents

- Board Workshop Risk Appetite Presentation
- Risk Appetite Register

Slide 1: Title Slide

(CISO): "Good morning/afternoon, everyone. Thank you for your time today. My name is [Your Name], and I'm the CISO. Today, we're going to have a critical strategic conversation about defining our company's risk appetite. This isn't just a cybersecurity discussion; it's a business discussion about creating a clear framework to guide our decisions and enable us to achieve our strategic objectives with confidence."

Slide 2: Agenda

(CISO): "I've structured our time today as a collaborative workshop. We'll start by establishing why this conversation is so important to our business. Then, I'll guide us through a four-phase framework. We will start by grounding our discussion in our core strategy, then explore our current risk culture, and then move into the core of the workshop: collaboratively defining our explicit risk appetite. We'll conclude by connecting our decisions to our governance structure and outlining clear next steps. My goal is for this session to be interactive and to result in actionable decisions."

Slide 3: The Goal: From Conversation to Action

(CISO): "So, why are we here? Every day, our management team makes decisions that involve taking on risk. But often, the 'rules of the road' for how much risk is acceptable are implicit, or just a 'feeling.' Our goal today is to change that. We want to move from that feeling to an explicit, board-approved framework.

"This framework will empower us to innovate with clear guardrails, to consciously decide which risks are worth taking to create value, and most importantly, to enhance this board's governance and oversight, fulfilling our fiduciary duty in a structured and defensible way."

Slide 4: Phase 1: Grounding the Discussion in Strategy

(CISO): "To begin, let's connect the concept of risk directly to our mission. This ensures our entire conversation is anchored in what matters most: our strategy. I'd like to open the floor to discuss three foundational questions."

(Facilitate the discussion, allowing board members to answer each question before moving to the next. Refer to a whiteboard or digital equivalent to capture key points.)

- "First, what are the key strategic objectives we are committed to achieving over the next 3-5 years?"
- "Second, to achieve these goals, what are the most critical business activities we must succeed at?"
- "And third, what are the major uncertainties or obstacles—both internal and external—that could prevent us from achieving these objectives?"

Slide 5: Phase 2: Exploring Our Current, Implicit Risk Appetite

(CISO): "Thank you. That gives us a clear picture of what we're aiming for and the uncertainties involved. Now, let's reflect on our existing culture and behaviors around risk. This helps us understand our starting point."

(Again, facilitate a discussion around each question.)

- "Thinking about past decisions, where have we historically been willing to be bold and take significant risks?"
- "Conversely, where have we always been highly cautious or risk-averse?"
- "This next question is critical for alignment: What does our current incentive structure reward? Does it encourage calculated, long-term risk-taking, or does it prioritize short-term gains?"
- "And finally, a question of capability: Do we feel we have the right people, processes, and data to effectively manage the risks that come with our strategy?"

Slide 6: Phase 3: Defining Our Future, Explicit Risk Appetite

(CISO): "This brings us to the core of our workshop. We've looked at our strategy and our past behaviors. Now, let's make a conscious, forward-looking decision about our risk appetite."

(Here, you will introduce the Risk Appetite and Tolerance Register template. It's helpful to have it displayed on screen.)

- "For each of the major risk categories you see here—Strategic, Cybersecurity, Operational, and Financial—I'd like us to discuss and agree on the level of risk we are

willing to accept to achieve our objectives. We can start with a simple scale of Low, Moderate, or High."

(Guide the board through each category, capturing their consensus in the register.)

- "Now let's add another layer. For the areas where we've indicated a 'High' appetite, what are the absolute boundaries—the guardrails—we should not cross?"
- "And for our 'Low' appetite areas, what does an unacceptable failure look like? What is the point at which we all agree the risk is intolerable?"
- "Excellent. Based on this entire conversation, how can we summarize our overall risk philosophy in a single, memorable Risk Appetite Statement?"

Slide 7: Practical Tool: The Risk Appetite & Tolerance Register

(CISO): "As you've seen, this register is the practical tool that captures our decisions and makes them operational. It's a living document that connects our high-level appetite statements to the specific, measurable tolerances management will use to run the business. Most importantly for this group, it provides a clear and simple dashboard for ongoing governance, complete with metrics, status, and management's action plans for any deviations."

"The link to this template is here for your reference. Management will own and update this document based on the outcomes of today's meeting."

Slide 8: Phase 4: Connecting to Governance & Next Steps

(CISO): "We've now defined our 'what' and 'why.' Finally, let's confirm the 'how'—how we will operationalize this framework and how the board will oversee it."

(Walk through the final set of questions to confirm alignment on the governance process.)

- "How will the board monitor that the company is operating within our newly defined appetite? I've proposed a quarterly review by the Risk Committee as a best practice."
- "What key metrics must management provide to this board quarterly to give you the necessary oversight? We will develop these KRIs based on the tolerances we've defined today."
- "Finally, are we all comfortable with the proposed RACI model, which holds management responsible for implementation and this board ultimately accountable for the framework?"

Slide 9: Next Steps & Discussion

(CISO): "Thank you for a very productive discussion. To ensure we turn this conversation into lasting value, here are the immediate next steps:"

- "First, management will take the outputs from today's workshop and finalize the draft Risk Appetite Statement and the Register. We will circulate this for your review before seeking formal board approval at our next scheduled meeting."
- "Once approved, we will cascade the framework to the senior leadership team to begin integrating it into their business planning and decision-making processes."
- "And third, we will establish the quarterly risk dashboard for this board's review, with the first report to be presented next quarter."

"With that, I'd like to open the floor for any final discussion or questions you may have."

Slide 10: Thank You

(CISO): "Thank you again