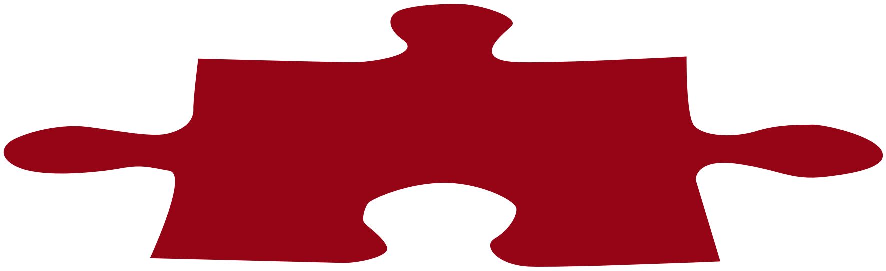
HIRING A CHIEF RISK OFFICER



BY ERIC HOLMQUIST

In coming years, the role of the chief risk officer, or CRO, will continue to be a vital part of a bank's management and governance structure. It is a common position within large institutions, though less so in smaller banks.

The CRO's role is not always well understood, however, and therefore it's often poorly defined. The result? Institutions that decide to hire for this position may end up with the wrong candidate. The reason is not that these institutions aren't effective at recruiting and hiring. Rather, they may not have been asking the right questions or they may have failed to define the type of person who would be most effective in the job.

Defining the Role of CRO

When considering a new hire for CRO, particularly when this person may be the first to assume the job, an institution must first outline the role and its responsibilities.

In addition to providing an ongoing risk perspective to the board and management on strategy and operations, the CRO—and the risk management function in general—has two primary responsibilities, both of which are defined in regulatory guidance:

- Be the architect of the bank's enterprise risk management (ERM) program and framework.
- Provide effective challenge to the first line of defense with regard to risk taking.

Accordingly, it is critical for candidates to have a certain amount of experience in building and supporting risk management programs and also be able to work effectively with all levels of management, the board, and regulators. The role of CRO is intended to be an executive position and should report to either a board risk committee (with a dotted administrative line to the CEO) or to the CEO directly. Ideally, this individual should not have other operational responsibilities or reporting lines.

For small institutions, however, regulators have shown some flexibility, realizing that the bank may not be able to support a fully independent function. However, the role should never be combined with a first-line business generation role (such as loan origination or branch operations). There is simply too much possibility for conflict of interest.

Some institutions will opt to create dual roles, such as CFO/CRO or chief credit/CRO. This approach can be successful, and regulators have shown some tolerance for small banks taking this approach. However, rather than combining roles, a better solution is to create a strong management risk committee that can serve as a "virtual CRO" until the bank is ready to fill a full-time position.

Once it begins the search for candidates, the bank should evaluate them based on their background and experience, both within the industry and in risk management practices. In addition to hands-on experience, the board should also be looking for the following:

- Strong "emotional intelligence" (this is quite possibly the most important attribute).
- Exceptional communication skills, both written and verbal.
- An attitude of collaboration, not an authoritarian style.
- A good, strong executive presence.

HAVING A BACKGROUND IN RELATED AREAS, SUCH AS INTERNAL AUDIT, COMPLIANCE, AND LEGAL, CAN BE HELPFUL, BUT IT DOES NOT AUTOMATICALLY TRANSFORM THE CANDIDATE INTO A GOOD PROSPECT.

Having a background in related areas, such as internal audit, compliance, and legal, can be helpful, but it does not automatically transform the candidate into a good prospect. In fact, such a background might make for a bad hire who falls back on previous focuses rather than the true CRO role. Similarly, while former regulators can bring tremendous experience and often the right skills, they would still have to adapt to a different type of role.

The bank will want to explore how candidates would transition from a role based on authority to one based more on influence. Often the best CROs come out of senior operational roles. These individuals understand the realities of the day-to-day business and only need to become skillful in applying risk management tools and techniques, such as providing effective challenge to the business.

Interviewing for a Chief Risk Officer

Once potential candidates have been identified, the bank should prepare questions to determine whether the candidate would 1) be a cultural fit within the institution; 2) possess the appropriate knowledge and experience to be successful in the CRO role; and 3) demonstrate the right temperament, communication skills, emotional intelligence, and perspective to effectively lead the institution's ERM program.

Part of this research could be covered in the standard interview questions, such as "Tell me how you handle conflict" and "What did you learn from your biggest mistake?" However, the questions that follow in this article are designed to probe further and gain insights into the candidates' experience in managing an ERM program, including their perceptions of risk management's role.

The questions could be answered by the candidates in written form. However, their answers will be much more genuine and representative if they are obtained in a live interview. Sometimes the most valuable aspect is not what the candidates say, but whether they can provide an immediate answer. Although certain questions may seem obvious, the responses—both in terms of what is said and how it is said—can be extremely revealing.

1. What is risk?

Surprisingly, this question is one that many CRO candidates are often the least prepared to answer. In fact, it catches many off guard because it seems so obvious. But the answers can be very insightful. In short, the most contemporary definition of risk (per the International Organization for Standardization's ISO 31000 guideline) is essentially "unexpected outcomes while in pursuit of our objectives."

Basically, for everything we do, there is a certain expected outcome. Anything that deviates from that expected outcome is technically a risk. Things could go better and they could go worse. It is the range of plausible alternatives that we have to consider, mitigating against the downside and being prepared to exploit the upside.

Strong answers: Those that are focused on unexpected outcomes, where the bank should be prepared to evaluate and mitigate the downside and seek to leverage the upside.

Areas of concern: Any answer along the lines of simply "stuff that can go wrong." While not technically incorrect, the answer is dated and narrow in perspective. It reduces risk management to largely a control exercise, when the goal is a more holistic view of balancing risk and reward.

2. What does risk management mean to you?

This follow-up question can yield a surprising array of disorganized and even rambling answers. Largely because the definition of risk management seems so obvious, candidates are not really prepared to describe it. But if they can't describe it, how are they going to defend it to the business units?

The most common response to this question is something like, "Do we have the right controls in place?" But this answer is spectacularly short-sighted, narrow, and out of date. It comes from an auditor mindset, where the controls are the focus. However, controls are not the CRO's primary focus—the risk is. In other words, a CRO should certainly care about which controls are in place, but care more about why they are there in the first place. Are they reducing the risk to an acceptable level?

A more contemporary view is that the bank has (or will have) established a framework for defining its risk appetite, and therefore "risk management" becomes the means by which the bank ensures that everything it does, from the strategic plan to execution, is aligned to the risk appetite and acceptable risk levels. It's about ensuring the bank is taking the *right* risks, not just imposing layers and layers of controls.

—

Strong answers: Ensuring that the bank has a clear strategy, has defined its risk appetite, has identified the key risks in strategy and execution, can evaluate whether the strategy and operations are aligned with the risk appetite framework, and has sufficient monitoring and reporting mechanisms in place to identify any meaningful changes in the environment. Bonus points for thoughts around culture, risk ownership, and accountability.

—

Areas of concern: Rambling answers, or answers that are focused on having the right controls to mitigate risk. These would likely indicate that the candidate either has very limited CRO experience, or is familiar only with less mature risk management programs.

3. What does enterprise risk management mean?

As a follow-up to the previous question, this one can yield some very interesting responses. If candidates are not really trained in risk management, they will have nothing left to say after describing "risk management" and will fumble around to come up with new material to describe enterprise risk management.

Typical responses are either a reworded version of the previous answer, or some version of "Well, that's just a different term for the same thing." The correct answer is, "Enterprise risk management means ensuring that our risk management practices cover *all* areas of the bank, across *all* of the risk types." This answer implies consistency and comprehensiveness, as opposed to risk silos.

—

Strong answers: Those responses that focus on clarity and consistency of the risk management framework (well-defined standards), universal application across the bank (people using the same tools and techniques), and ensuring that risk is evaluated and addressed across all areas of the bank, not just "high risk" areas.

—

Areas of concern: If the candidate is unable to define the term, provides a reworded version of "What is risk management?" or waves the question off as "just terminology."

4. What are the core elements of a sound ERM program?

Answers to this question can take many forms, covering a variety of elements and

in no particular order. However, a strong ERM program has core elements, and an experienced CRO should be able to answer this one immediately.

—

Strong answers: 1) A good governing risk management policy and supporting policies; 2) clearly defined roles and responsibilities, supported by regular training; 3) a strong risk governance structure, which can look different depending on the size and complexity of the institution; 4) a method for conducting comprehensive risk assessments, both thematically (such as "fraud") and horizontally (for example, "enterprise-wide for all types of risk"); 5) well-defined methods for risk monitoring (like KRIs) and reporting; and 6) a documented, tested incident-response program. Much more could be included, but these basic elements are critical. Bonus points for thoughts on culture, tone from the top, board engagement, and a good change-management process.

—

Areas of concern: Answers that hit on some or all of these areas but take a lot of thought to work through. This question should be the easiest one to answer, assuming the candidate has actual experience managing mature ERM programs.

5. What are the three lines of defense? How does each fit into a holistic ERM model?

This question should be a softball for anyone who has read anything about risk management in the last 10 years. Simply put, the first line of defense—which is the revenue-generating business units, the supporting back offices such as loan operations and deposit operations, and finance—"owns" the risk. In other words, these functions are ultimately responsible for the risk-taking decisions and the consequences of those decisions. Accordingly, they are responsible for managing risk to within acceptable tolerance levels.

The second line of defense includes independent risk management, compliance, and others.

This line owns the frameworks for risk and compliance programs and provides effective challenge to the first line.

The third line of defense—internal audit—provides attestation on the control environment. That is, "Did we do what we said we would do?" Anything that veers too far off these definitions means that the candidates don't understand the three lines, or they may have taken on their own interpretation of what the various roles are or should be.

THE CRO—WHETHER SERVING AS A ONE-PERSON RISK MANAGEMENT DEPARTMENT OR SUPERVISING A LARGE GROUP—IS THE LEADER OF THE BANK'S SECOND-LINE FUNCTION.

A follow-up question can certainly be asked along the lines of "Do the three lines work?" or "Should there be other lines?" There's no real right or wrong answer, but it's possible to sometimes unearth any rogue views, often rather passionately held by candidates.

—

Strong answers: Those responses that support the concept of the first line as risk owner, the second line as program architect and effective challenge, and the third line as independent validation. Bonus points for an understanding of embedded risk managers within the first line who serve as primary facilitators and liaisons between the teams of the first and second lines (a situation more common in large institutions).

—

Areas of concern: Aside from any strange views on how the three lines should be defined, other answers may reflect certain biases based on background and experience. For instance, references to the second line conducting control testing may reflect more of an audit background. Any reference to the second line being an approver of risk-taking decisions or having any risk ownership would be extremely outdated and a key concern, given that this is no longer considered standard practice.

6. What is the role of the chief risk officer?

This topic may have already been covered sufficiently by the prior question. If not, it should be asked. It is critical to understanding the candidates' view of the role for which they are applying. In short, the CRO—whether serving as a one-person risk management department or supervising a large group—is the leader of the bank's second-line function. It is key that candidates understand that their role is to design and oversee the risk management program. This means application of a strong architecture and the ability to provide effective challenge to the first line.

—

Strong answers: Responses grounded in the design and challenge role are ideal. Partial credit for references to the "corporate conscience," someone who can see the "forest for the trees," or a connecting point between staff, management, the board, and regulators.

—

Areas of concern: Any reference to levels of authority. This is an immediate red flag. CROs who see themselves as the "risk police" will only foster a culture of fear, blame, and lack of transparency and accountability. Thank these candidates for their time and move on to the next one. References to "protecting" the board, CEO, and others may also be a concern, and the candidates should make clear what they mean by that statement. Meanwhile, any answer that emphasizes "satisfying regulatory expectations" is also a red flag because it may reflect a view that risk management is largely a compliance exercise.

7. How would you go about implementing an ERM program?

This is a terrific question to ask, both for the answer and how it is given. For starters, if candidates have to think about the answer for a long time, then they likely don't know it and probably don't have the right experience. A candidate who will be learning on the job is just introducing another level of risk.

The specifics of how someone might go about implementing a program can vary. There is no absolute "right" way. But some insights can be gleaned from the answer. If the response starts with things like policy, board and senior management support, and the bank's strategy—that's a good thing. It shows a good, top-down view, which is always the best place to start. If candidates go straight to department-level risk assessments, their response is less ideal. It means they bring more of an audit mindset and will approach the program in a more bottom-up fashion.

Alternatives could include leading through training (good), defining a clear framework first (very good), building out a big team (questionable, but probably not good), or forming a risk committee (a good thing to do, but not necessarily the first thing). In general, the sequence should be 1) learn about the bank; 2) develop a framework; 3) educate the top of the house and gain its support; 4) implement the framework elements; and 5) maintain a strong monitoring, reporting, and response process that can be reevaluated as needed.

—

Strong answers: Those responses that show some experience with designing and implementing a strong framework. The specific items and sequence of events are probably less important than whether the answer is quick and succinct. Bonus points for giving priority to understanding what the board and senior management want, as well as their view of risk strategy, risk appetite, and risk management.

—

Areas of concern: Any response that requires the candidate to think long and hard. Answers that focus on bottom-up activities, such as departmental risk assessments and controls testing, are key red flags. Obviously, answers like "I would buy a book" or "I would go to a conference" should pretty much end the interview.

8. How would you develop a risk appetite framework?

How the bank implements a risk appetite framework can take many forms. What's more critical is whether the candidate actually has experience designing such a framework and is prepared to assist the bank in developing one (assuming that one doesn't exist).

Ideally, the candidate should speak to risk appetite in relation to the strategic plan, as well as to the processes in place to achieve that strategy. As a side note, the candidate may have a perspective on whether risk appetite should be defined by management and be reviewed and approved by the board (the correct view) or whether it should be defined by the board and imposed on management (the incorrect view). The latter perspective does not represent a good governance role, and it will never foster a sense of risk ownership by the senior management team.

—

Strong answers: Responses that emphasize the perspective of the board and senior management are ideal, particularly those with an emphasis on strategy. The candidate should focus on helping to facilitate a collective view and consensus on acceptable risk levels—and be able to help management identify suitable risk metrics to measure performance against the stated risk appetite.

—

Areas of concern: Inability to answer this question quickly and succinctly is a key red flag. It likely indicates that the candidate may have heard of or been subject to risk appetite statements and metrics, but has never actually facilitated the process of developing them. Answers that jump straight to identifying KRIs also indicate that the candidate probably doesn't have experience in developing risk appetite statements.

9. What do you see as the role and function of a board risk committee?

A lot can be said about the role of a board risk committee, but the answer to this question should focus on oversight of the bank's risk management program and key risks. The candidate should be able to distinguish between an audit committee and risk committee and also be able to discuss committee membership, appropriate subcommittees, and key agenda items. The focus should be on a forward-looking view of the bank and its risk profile, not on discussing what has been done in the past or engaging in micromanaging.

Strong answers: Responses that emphasize a forward-looking view, oversight, governance, and challenge are all strong and indicate a candidate's experience. Bonus points for helping set "tone" and encouraging a culture of transparency and risk ownership.

—

Areas of concern: Answers that focus on roles that are clearly the responsibility of other groups, such as audits and lending decisions, are weak. The emphasis should be on where the bank is going and not on what has already been done. Any reference to managing details (for example, day-to-day activities or design of process or controls) is a real concern.

10. What do you see as the role of a management-level risk committee?

A management-level risk committee should have the same basic texture as the board risk committee. The key difference is that, at the management level, the discussions should be much more hands-on, as opposed to the "Should we do it?" discussion.

A management committee will also evaluate things like lessons learned from unexpected events, key initiatives, the results of risk assessments, and the health of the risk management program overall. But the view should still be forward looking, not backward looking.

Membership should come from the executive level. A committee staffed with more junior and middle managers will have difficulty addressing issues of strategy and policy. Issues that are primarily operational are better left to an operational risk management committee.

The risk committee should also serve as a funnel for reports from other committees, such as the compliance committee or credit committee, and be prepared to summarize risk information in aggregate before reporting to the board risk committee.

—

RISK MANAGEMENT IS BOTH STRATEGIC AND OPERATIONAL, BUT ONE USUALLY IS EMPHASIZED OVER THE OTHER. IT DEPENDS ON THE INSTITUTION AND ITS RISK MANAGEMENT PHILOSOPHY AND FRAMEWORK.

Strong answers: A candidate stating that the management-level risk committee is similar to the board risk committee indicates a forward-looking view of the bank. It comprises executive members who have decision-making influence on strategy and policy. And it serves as a parent committee to potentially numerous other committees covering specific risk areas, each representing subsets of the bank's overall enterprise risks.

—

Areas of concern: Any view that is operational in nature or includes a focus on management details—such as design of processes or controls, or being "in the weeds" on decisions that can easily be left to other working groups. Also suspect are any views implying that the committee serves in a compliance capacity, to simply ensure that the bank maintains its risk management processes.

11. What do you see as the board's role in the risk management program and processes?

Simply put, the board's role here is oversight. The board is a governing body and should have very little involvement on a day-to-day basis. Its role is to oversee the bank's risk management program and to work with the senior management team to understand key risks, identify emerging risks, and ensure cohesion between strategy and risk management.

—

Strong answers: Anything that reflects the board's oversight role as part of a general governance framework.

—

Areas of concern: Any references to hands-on management, direct involvement in day-to-day risk management activities, or program or control design.

12. Do you see risk management as strategic or operational?

This is partly a trick question—or, at a minimum, a poorly phrased one (bonus points for recognizing that, but minus points for pointing it out). Risk management is both strategic and operational, but one usually is emphasized over the other. It depends on the institution and its risk management philosophy and framework. Nevertheless, risk management starts right at the point of setting strategy and exists throughout all areas of the operation.

—

Strong answers: Any form of "both"—with the ability to articulate why.

—

Areas of concern: Any form of one or the other, or any ill-formed attempt to justify the answer, which accidently ends up back at some version of "Well, I guess both."

13. Do you see risk management as proactive or largely reactive? Why?

This is a slight twist on the previous question. There really isn't a right answer, but the fact is that risk management, when done effectively, should be proactive. The practicality is that many risk management activities are in fact reactive. But if the program is operating as it should, the bank will have information that helps when making proactive decisions.

—

Strong answers: Any version of "both" supported by a credible rationale. Bonus points for pointing out that the industry in general is working to make risk management more proactive—with more offense and less defense.

—

Areas of concern: Any version of "No, largely reactive." Also, any version of "Well, now that I think about it—yes, both."

14. Which areas do you believe should report to the CRO and why?

This question is under debate and people have different perspectives, so it would be good to learn the candidate's view. At a minimum, this would include everything having to do with the bank's ERM program and the compliance function. Other areas commonly part of the risk management organization include model risk management, vendor management, and sometimes the CISO and even chief credit officer (although there are competing schools of thought on this last one).

Again, this issue is for each bank to navigate in coordination with its regulators. So the most useful aspect of the question will be to learn whether the candidate has a perspective that would reflect related experience.

—

Strong answers: Those responses that can describe and defend which areas are most logically part of the risk management area.

—

Areas of concern: An inability to provide a clear perspective one way or another—or any reference to first-line operations (such as IT or operations) reporting to the CRO.

15. Who do you think the chief risk officer should report to?

Contemporarily, the only correct answer is that the CRO should report to either a board risk committee (with a dotted administrative line to the CEO) or to the CEO directly. Any alternative answers are worth exploring to understand the candidate's rationale.

—

Strong answers: Board risk committee or CEO.

Areas of concern: Anything else—or expressions of uncertainty, including "Well, where do you think it should report to?"

16. What approval authority should the CRO have? What veto authority?

This is another trick question. CROs should not have approval authority outside their own departmental P&L (for example, consultants, software tools, and so on). For new initiatives, it is not uncommon for CROs to sign off that the risk management "process" was followed, but they should not be approvers of initiatives. Otherwise, they become part of the risk-taking decision, which is the role of the first line.

This approach represents an evolution in the CRO role. Depending on how long candidates have been in the industry, they may still hold to old methods that gave the CRO veto authority. But a CRO who is the chief "no" officer will always struggle to create open dialogue and collaboration. CROs are

better off leading through influence, not authority.

—

Strong answers: Any version of "Only of their own P&L."

—

Areas of concern: Any answer that describes specific approval or veto authority over business decisions.

17. What should happen if the CRO disagrees with executive management about risk management?

The answer to this question should always be as follows: First work with senior management to discuss the issue and see if a consensus can be reached. If the CRO still feels that management is pursuing a strategy or processes that deviate from the agreed-upon strategic plan or risk appetite, he or she should raise these concerns with the CEO and then with the board (or board risk committee, if one exists). Ultimately, it's up to the board to determine if management's actions are acceptable.

—

Strong answers: Those that generally follow the escalation path described above are ideal.

—

Areas of concern: Answers that follow a more authoritarian path, where the CRO becomes the final say, or any views that are highly problematic and inconsistent with current practices.

18. How does effective risk management improve the bank?

In other words, does the bank ever get its money's worth, or is risk management just a compliance exercise? This is a highly subjective question that could lead to lots of discussion and offer insight into the candidate's actual experience with designing a risk management program and building efficiency into the risk management process. This is a capability the bank really wants in its new CRO.

—

Strong answers: Basically, any response that would indicate the candidate has looked at the elements associated with a risk management program and has spent time thinking about how to minimize impacts to the business while also creating business value.

—

Areas of concern: If the candidate has to think at length about this question or tries to manufacture answers on the spot, he or she probably lacks related experience.

19. What do the regulators expect for a bank of our size? *(This may require some description first of the institution's business model, product and service mix, and so on.)*

Possible answers to this question will depend heavily on who the bank's primary regulator is, the size and complexity of the bank, and other factors. The useful part of this question is not really the answer. It's whether the candidate has an answer.

—

Strong answers: Anything that shows some familiarity with regulatory expectations, even if that includes qualifiers based on differences between your institution and the candidate's former bank.

—

Areas of concern: An inability to even address the question, which may indicate very limited past involvement with regulators. Another concern would be answers that simply don't make sense for an institution of your size and complexity—that is, a one-size-fits-all mentality.

20. Do you lean on any one particular framework as a basis for an ERM program?

The more common frameworks are the aforementioned ISO 31000 and the COSO ERM. Both have strengths and weaknesses, and neither has enough information to support a fully developed ERM program.

Strong answers: The ideal response will reference multiple frameworks and then propose one that uses the best elements of each. But the framework should be appropriate to specific circumstances and how the bank seeks to manage risk.

—

Areas of concern: A candidate being strongly aligned with one particular framework isn't inherently bad, but it may not be good. The best risk practitioners learn from various frameworks and ultimately implement something appropriate for the specific institution.

21. How do you see risk management evolving within the industry?

This question really has no correct answer. People will perceive risk management evolving in different ways, but the candidates' ability to at least articulate a perspective would yield insight into whether they are current on general industry practices.

Some ways in which risk management is evolving include the following: 1) less emphasis on building programs and more emphasis on "tuning," ensuring the program is forward looking and creates real business value; 2) continued clarity around the three lines and their specific roles and responsibilities; 3) better alignment between strategy and risk management; 4) improvements in ongoing reporting, focusing on the issues that really matter; and 5) more real-time information versus lagging metrics.

—

Strong answers: Generally, a response that shows the ability to provide a perspective. Beyond that, being able to credibly describe ways in which risk management is evolving, whether based on the items above or other thoughts.

—

Areas of concern: Not having a perspective is cause for some concern. A good CRO should always be in touch with industry trends and best practices. Beyond that, any answer that sounds manufactured or that could be construed as a best guess.

And Now a Word from the Candidate…

Interviews are a two-way street, and there are some questions that an experienced CRO should be asking of the bank. The following questions offer a good indication that candidates understand the position and that they are considering how they will fit the culture and be able to add value.

- How does the bank define the position?
- What are the states of the current ERM and compliance programs?
- How was the existing program designed? Was it developed internally or with outside assistance?
- How has it evolved?
- How does the board feel about the current ERM program?
- How would the bank describe its risk culture?
- Has the bank been complimented or criticized by its primary regulator on the risk or compliance programs?
- If this is a replacement position, how was the prior CRO successful? How was that individual less than successful?
- How would the bank define a successful risk and compliance program?
- If this position is new, what prompted its creation?
- How will my performance be measured and evaluated? Are there set criteria?
- What staff and functions would be reporting to the CRO?
- Is the CRO responsible for all risk types or only some? (Hopefully, the answer is the former.) If it's the latter, who has oversight of the other types of risk?
- Who does this position report to?
- Is the CRO involved in the strategic planning process? (The answer should always be yes.)

In the end, it is difficult to know whether a candidate will be the perfect CRO. But asking questions that allow candidates to articulate their view of risk management and the CRO's role can go a long way toward ensuring the best possible candidate—and success for the bank's risk management program. ®

ERIC HOLMQUIST is managing principal at Capco. He can be reached at eric.holmquist@capco.com.