Are you old enough to remember the game Twenty Questions?

Wikipedia's description:
"Twenty Questions is a spoken parlor game which encourages deductive reasoning and creativity."
Remember the standard questions? Is it bigger than a breadbox? animal or vegetable? Admittedly dated; just what the heck is a breadbox anyhow and how big might it be? Today's equivalent? Is it bigger than an XBox 3? Is there an app for that?

If you have just been named as your institution's risk manager or chief risk officer (CRO) you probably have at least 20 questions, as do the executives who appointed you. And like the game, the questions are fairly standard from bank to bank.

Question 1: What is the CRO's job description? It is perhaps best stated as "oversight of the institution's enterprise risk management process and its myriad disparate risk silos". But the day-to-day requirements call for questioning everything.

Consider this. You have just been made chief risk officer for the frat or sorority house at the state university. What is your role on Saturday night? Checking IDs at the front door or looking for people sneaking in the back door? Checking what goes into the punch? Bed check? Out on the front lawn keeping an eye out for the campus police? You're responsible for all that and more. Pretty much a lose-lose position. Do your job and everyone views you as the conservative campus curmudgeon; Triple-C to your friends. And if something goes wrong, you're to blame.

Which brings us to Question 2: As Ford has famously framed the question; What is Job 1?
Job 1 is probably asking these questions and implementing structure and process to build the accountability, responsibility and clout that gives you, as the CRO, both a seat and a voice at the executive table.

The consideration of your executive role, or at least your "mesh" with the executive team spawns questions 3 through 5: What does the CRO do that the CEO does not do? What is your authority day to day? What is your responsibility as whistle-blower? For small institutions, the CEO is the CRO. Period. "The buck stops here" and all that. All major decisions emanate from the corner office; branching, C-Level hiring decisions, corporate strategies, and so on and so on. The CRO is generally out of that picture, transforming many risk positions into mere compliance administration. So, is your authority characterized as pro-active day-to-day or reactive as whistle-blower? It's a mix of both.

Questions 6 and 7 dovetail. Can you be effective if you are home-grown? What if you already know these people and this business model? This is really an important and often over-looked issue. Many institutions have created the risk position around the individual seemingly best suited to the role. The COO, the audit manager, the compliance manager,

the CIO, or perhaps a soon-to-retire individual who can be moved aside to make way for a new strategic hire. The concept of risk manager has been likened to police internal affairs. Once you take on that internal policing role, you are required to sever all previous "friendliness". I think that's too severe, but how do you jump up the organizational chart to a position that needs to ask critical questions of lending or finance? Aren't the respective managers the experts? The risk manager's autonomy, however, is entirely similar to that of our traditional internal audit department.

Questions 8, 9, 10 and 11: How strong a voice must CRO have? How senior? With a seat at the executive table? How wide should the risk manager's responsibilities and authorities range? My answers to the first three? A CRO needs a very strong voice as a senior manager with a key seat at the executive (and perhaps board) table. These three qualifications set the tone for establishing the range of responsibilities and authorities.

As to question 11, if the role of the CRO is based on an enterprise-wide risk management philosophy, doesn't this set of questions answer itself? Global reach, and the awareness and ability to delve into each area of the institution are important. Perhaps most important is the ability to see how all the functional areas mesh. In this capacity, the CRO is perhaps the keeper of the business and process flow integration blueprint.

Here's an example of responsibility, role and reach. Credit concentrations are a hot topic. The OCC published new guidance in December, 2011 and policies, procedures and reports attendant to the issue of concentrations of credit are being re-examined and reconsidered. Who's responsible? The senior lender. For what? Policy, procedure and metrics. What is our CRO's role here? If the CRO merely monitors that the lending group is aware of
the new guidelines, has reviewed policies and procedures in light of the new guidance, and has created and presented reports with properly calculated concentration metrics, then we have taken on the compliance admin moniker we are being careful to avoid.

This is where the CRO can start asking questions. What does this analysis tell us? Are the metrics consistent with our strategies? With our budget? With our incentives? Do we need to be worried? Do we need to change our approach? Which concentrations should give us pause? In short, did we merely conduct the analysis for regulatory appeasance or have we reached a moment of affirmation? Or conversely, have we reached a "so now what" moment? If the CRO has a strong voice, speaking from a senior position at the executive table, this questioning should be expected and respected.

Question 12: To whom do you report? This is one of those functionally-reporting- versus-administratively-reporting-with-a-dotted-line-in-the-orgchart moments. The key factor, however, is independence, and we should look to traditional structures for internal audit managers as guidance.

Question 13: If no real internal auditor is designated, who is it? You? Smaller institutions in which the internal audit function is completely outsourced struggle with this question, and the appointment of a risk manager may help with this dynamic. The risk manager is not an auditor, but his/her role very naturally may assume the audit liaison role; with internal, external and regulatory audits. The risk manager can logically take over the audit issues tracking function, reporting typically to the Audit Committee (or Audit & Risk Committee as some banks have re-energized and re-chartered).

Question 14: What is the risk manager's relationship with the Audit Committee? Direct report, for starters. And similar to the leadership and choreography role played by audit managers, the risk manager may "shepherd" the meetings; scheduling, planning, and report distribution.

Questions 15 and 16 represent my audience participation moment when doing "Twenty Questions" as a presentation. Would you change the Audit/Risk Com dynamic/charter? How? Discuss.

Question 17: Assessing risk – what does "high-moderate-low" mean in your world? Risk appetite is defined as the amount of risk an entity is willing to accept in pursuit of value. How is this assessed? Risk, like beauty, is in the eye of the beholder and the question of consistency always arises. Who ultimately referees? Somebody has to! Each functional area views risk through the lens of their unique functionality, making enterprise-wide assessment complicated. High-Moderate-Low is subjective, judgmental and fickle. What's the measuring stick or key metric? In March, 2011, the OTS issued a CEO Memorandum addressing capital management. It turns out to be a terrific risk management publication in my opinion. In addressing capital management and suggesting that banks establish their own capital targets (the presumption being that the targets be "tougher" than regulatory rules), a list of enterprise risks is delineated, with capital ratios as key metrics; our measuring stick. All risk managers should have this memorandum in their toolkit.

The risk exercise is often clouded by traditional biases and "over-weighting". Reputation and compliance risk are both terrific examples of over-cooking. Relatively small risks that might result in a handful of disgruntled or lost customers and similarly, small risks that are easy targets for examiners (HMDA and flood insurance compliance come immediately to mind) get lots of ERM attention and weight. Meanwhile, unmonitored problems may lurk. What about an institution that has poor employee performance review files coupled with sloppy and ill defined termination procedures? Wrongful termination lawsuit lurking? More impactful than HMDA violations? Any of the audit budget directed to this subject? Why not?

Question 18: How do you guide your bank, staff, auditors for a consistent approach to risk definitions? This is difficult to define within an individual bank, and equally difficult for the entire fleet of risk consultants, risk system providers, external audit firms, internal audit firms and regulatory examinations privy to the institution's risk environment. Careful definitions that capture relativity should provide a working model from which thoughtful risk discussions may spring. Because, in the end, the risk designation is a collaborative metric, serving as the starting point, and then memorializing the risk analysis/discussion with an end result - or at least as much of one as a risk assessment might provide.

Question 19: How do the Risk Committee or Audit Committee weigh in on risk appetite? Ideally, they set the parameters of the H-M-L red-orange-green dashboard. Risk appetite and risk rating definitions at the ERM level may provide interesting Board retreat subject matter. And if the Board has set the definitions, the risk manager need only interpret and enforce.

Question 20: What if risk management becomes merely compliance admin? This is the pitfall facing and confounding risk managers and CROs. Institutions are establishing top level risk positions, only to pile on so much risk minutiae as to blur the vision. How does the risk manager push back? The answer is now often found in shifts in organizational architecture. Meet the Risk Department! Compliance, BSA, and other risk areas may now report into a CRO as an overall consolidator, a clearing house for all things risk.

To end where we began, our Wikipedia description describes a game that "encourages deductive reasoning and creativity." Thinking of the CRO role, I might change that to deductive questioning and creative re-focus on the results of risk assessments; not the "doing" or forensics of risk assessments, but rather the informative gathering of the implications of what the risk assessment discovered or uncovered.

This article was published in Maine Community Banker, 1st Qtr. 2012 and Connecticut Banking, 2nd Qtr. 2012