5

Effectively Assessing and Managing Ethics and Compliance Risks

Insight from SNC-Lavalin in Identifying and Prioritizing Key Risks Across the Company

Interview with:

Amee Sandhu

Regional Integrity Head, USA & LatAm, and Sector Integrity Officer, Mining & Metallurgy

SNC-Lavalin

Walid Awad

Governance, Risk Management & Controls

SNC-Lavalin

As we speak with c-suite leaders across a variety of companies and ask about the risks they face and are most concerned about, risks relating to third parties inevitably come up first. Whether from suppliers, agents, distributors, partners, etc, working with third parties is both a critical part of a successful global companies and the source of much frustration and sleepless nights. In the following article we explore the ways companies can manage the myriad of enterprise level risks that arise from working with third party organizations.

E: I understand SNC-Lavalin is going through the process of simplifying its ethics & compliance risk matrix in order to create a more effective risk assessment and mitigation program. Could you please share a bit more about this and what prompted the review?

SNC: Our purpose in the review was primarily to update our Risk Assessment process to take into account both the changing landscape in which we operate and to recognize the growth in our policies, training, senior leadership involvement, and company re-orgs. Finally, like all functional departments, we need to ensure that we are always efficient, especially in terms of what we ask of our business teams.

Our ethics and compliance function (now called Integrity) was created in 2013, and our first formal risk assessments in the business took place in 2014, when we held 25-26 separate ones. In 2015 and 2016, we also held 25-26 each year, covering different business and regions, as well as corporate functions.

By 2016, 2017, etc., our Integrity Program had developed into such a mature department, that many of the risks that were being identified had already been mitigated. We had responded to many of the identified risks by implementing a comprehensive set of policies, training, senior leadership engagement, metrics and a road map going forward.

Because we started our Risk Assessment process so soon after we created our Ethics and Compliance function, in the early years, the risk workshops ended up serving a dual or triple role: that they also served as a way for senior management to show their commitment to ethics and compliance values – doing 25 a year meant hours and hours of management time across the company. It also served as a workshop environment for leaders to discuss what ethics risks their business units were facing.

Now, Integrity is a key topic that is built into our so many of our trainings, communications, processes, values, meeting, etc., so that we don't necessarily need the venue of the risk assessments workshop to educate leaders on what ethics risks are.

As ethics has become such a front and centre part of our business, we've optimized the risk assessment process to focus on the areas of the business that are faced with various internal and external challenges and market forces. In addition, while we are doing fewer formal risk assessment, being a project based company, we do recommend that specific project risk assessment include ethics risk topics on their risk registers.

Our Enterprise Risk Management process also engages our senior leadership teams and board. The executive committee will review the outcome of our functional and regional risk assessments and provide input on the risk tolerance for each risk theme. This annual exercise is a key component of aligning our overall strategic objectives with our risk management practices. All of this is reported to the board of directors who have ultimate oversight over our risk profile. In pursuit of our strategic objectives, we keep top of mind that due consideration must be given from a risk management perspective so that we can operate within our set boundaries.

Like any other function, we are always looking at ways to be more efficient and work more collaboratively with our business teams.

E: What are your goals in the review, and what does success look like?

SNC: Our goals in our review would be to ensure we have a robust and efficient process that identifies any new risk that emerges while also continually monitoring currently mitigated risks for changes. These new risks can emerge because we are doing work in a new country or region, or with a new type of customer, or with a new product line, or due to a new law.

Success looks like:

- Identifying the risk;
- Quantifying and prioritizing the risk (i.e., reputational risk? financial risk? national, regional or international impact? low, medium or high risk?);
- Identifying risk owners;
- Determining mitigations and owners of the specific risk mitigations;
- Follow up process to ensure accountability; and
- Reporting to Board / Executive to ensure accountability on progress.

E: Who "owns" the risk matrix at SNC? Is it an individual in the compliance team, the entire team, executive leadership, etc.? I.e., Who owns the Integrity risk assessment process?

SNC: Our Integrity function, and specifically our Chief Integrity Officer, would be responsible for ensuring that the ethics risk assessment process is implemented. But there is visibility at the Board and Executive levels.

As per my comment in the last question, who owns the risk will depend on what the risk is. Sometimes there will be more than one owner for parts of the risk.

For example, for Conflict of Interest risk, the Chief Integrity Officer would own the risk for reporting purposes, however many of the mitigations are reported to the HR Committee of the board of directors since this risk can only be adequately mitigated through a joint effort with the HR function.

Risks ownership is broken down based on the nature of the risk and will reside with the senior leadership team to ensure accountability. The board will have oversight of these risks to ensure that management is executing the mitigation action plans.

This is a great question, because one risk can be broken into a few different risk mitigations, where responsibility could and should be housed in different parts of the company. But it does require a great deal of clarity – i.e., who exactly is responsible for what aspect.

E: How do you identify and prioritize risk assessments and reviews? Do you discuss internally, have external benchmarks, etc.?

SNC: For the Risk Assessments themselves: Our simplified approach is now to hold one in person for each corporate function through the ERM risk assessments and to hold regional ethics and compliance assessment virtually with our various regional hubs (i.e APAC, Europe, etc.). This allows us to adopt a bottom-up and top-down approach by gaining insights from corporate as well as our employees in our various regions. Ultimately, this creates a more holistic approach to risk management and in identifying, assessing, prioritizing, mitigating and monitoring our ethics & compliance risks in domestic and international markets.

We currently hold 6 regional Integrity risk assessments per year, and an additional 6 for our corporate functions through the ERM process. This simplified, yet comprehensive approach, brings us to a total of 12 annual workshops.

For Risk Identification:
We use risk workshops where we take the round table approach (i.e., brain storming sessions), with some key topics (i.e., business partner risk, government official risk, etc.). This brainstorming approach, but using key topics, is the same approach we use for our project risk reviews (i.e., but in the project context, it could be schedule risk, subcontractor risk, etc.).

"OUR GOALS ARE TO ENSURE WE HAVE A ROBUST AND EFFICIENT PROCESS THAT IDENTIFIES ANY NEW RISK WHILE CONTINUALLY MONITORING MITIGATED RISKS FOR CHANGE."

For Risk Prioritization:
At SNC-Lavalin, we already had a developed program for project risk reviews, so we were able to build and use the risk level tests. I.e., we have a consistent approach to determine if a risk is low, medium or high based on a formula of potential frequency and potential impact.

E: In a brainstorming session, if a group of individuals comes together to identify the myriad of ethics & compliance risks that a multinational company like SNC faces, the list could become endless. How do you decide which are the key risks, and is there a right number of risks worthy of assessing deeper as an organization? (Is it 10, 50, etc.)

SNC: In fact, this has been our experience. It certainly was more the case when we started our Risk Assessment process.

We work with our Risk department professional to co-lead our sessions, where possible. They are quite instrumental in keeping the group discussion on track in terms of identifying actual risks, as opposed to theoretical risk that may apply to another company or another type of business.

For example, in one of our early risk assessments in 2014, this risk was added to the risk register "the risk of our employees breaching the code of ethics". In hindsight, it was too generic of a risk– a risk needs to be more specific.

But if we keep that risk for the purposes of an example, it leads into another question: and that is, what principles do you apply in order to retire a risk? From a risk philosophy, you are not trying to eliminate risk.

Instead, you are trying to reduce or mitigate risk to a level your company deems tolerable. Risk in business can never be eliminated. In practical terms, if the risk is of someone breaching the code, you need to ensure your hiring approach, on-boarding of new employees, training, internal processes, Tone from the Top of leadership, and employee discipline processes are all strong. The way in which a risk is mitigated also differs greatly. Depending on the nature of the risk, it may be more pragmatic to reduce the likelihood of the risk materializing. In contrast, you may have a mitigation strategy which instead reduces the impact (reputational, monetary, etc.) of the risk if it materializes.

In an ideal world you would want both at all times, however in reality it is not always so simple. We therefore take a multi-functional approach to mitigate risks in order to ensure that a risk is not assessed in isolation, but rather through the various perspectives it may impact (i.e the Conflict of Interest example mentioned earlier).

E: How frequently does the organization assess its key risks, and what's the right frequency for undertaking assessments of these key risks?

SNC: Given the size, global presence, and organization of the company, we use a cycle of once a year. And in fact, it can take a year to put in place appropriate risk mitigations (i.e., write a policy and create new training and management metrics surrounding such policy).

However, like all companies, we also have many opportunities throughout the year to discuss other emerging risks. For example, we would also revisit risks when new legislation comes into force, if an investigation reveals something in one specific scenario that prudence dictates should be examined more broadly. Another example is if Internal Audit audits part of our Integrity program, and raises a gap in process, etc. We would not wait until the annual Risk Workshop process to discuss or put in place a response.

Also, even though the risk assessments are held formally once a year, there should be regular reviews to confirm progress, with status reports going to the Board or Executive.

A smaller company or a company that is trying to drive cultural change after some kind of negative Integrity event may wish to have more frequent assessments .

E: What challenges have you discovered as part of the risk assessment process, or what advice can you give to other organizations looking to simplify their own risk matrixes?

SNC: Another great question! And this is where I believe we can offer a lot of insight, as we really have immersed ourselves in the Ethics risk assessment topic since 2014.

The challenges that we have experienced, and that we imagine many others companies could face are the following:

A) When starting out it is better to incorporate this directly into an ERM (enterprise risk management) process, if your company already does ERM.

The benefits of doing it that way are:

i. You are sitting down with your business team(s) once instead of in a duplicate process, which always builds goodwill. You can make one longer workshop, instead of holding two separate ones with the same group of people.

ii. You demonstrate that ethics and business should be thought of analysed together, and not separately. This is how you want your organization to think about business risk. Having a separate session creates a false distinction between ordinary business risk and ethics risk.

iii. Related to i & ii , there is a built in efficiency with having the company follow one type of risk control system, rather than having multiple ones. This allows greater efficiency, and greater impact and more time to discuss at senior-most levels.

But what if you don't have an ERM yet? Don't wait for one. Go ahead with the ethics risk assessment process, and then adapt later once you have an ERM.

B) Another challenge we faced initially was how to get attendees at a risk workshop to understand and characterize an ethics risk, if it was their first experience doing so. While all opportunities to educate are valuable, it could mean that you spend more time than planned on the intro and principles and risk identification, but then run out of time for discussing and agreeing on risk ownership, mitigation plans, setting deadlines, etc.

C) Distinct but related to b) We chose to start off with key categories to help guide our initial workshops. I.e., Conflicts of Interest, interactions with government officials, business partners, anti-competitive behaviour, intellectual property, etc.

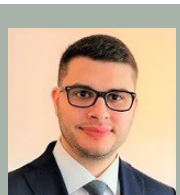
Note that if you provide the "checklist" of topics, it can result in each topic being discussed equally, instead of focusing discussion on the key ethics risks for that particular segment of the business. For example, if Business Unit A does not have any Intellectual Property that they use in the execution of their work, then while it may be interesting to discuss theoretical IP risks their business may face, if you are facing time pressure, it's better to move on to the next risk category, and spend the time on an actual risk facing them.

D) Trying to do too much. This can include having too many risk workshops leading to too many risk registers to keep track of. Focus on the key aspects first if you are starting off, then you can build on it as your program matures.

E: Thank you for sharing your insight with us!

About the Expert

Amee Sandhu is Regional Integrity Head, USA & LatAm, and Sector Integrity Officer, Mining & Metallurgy for SNC-Lavalin



About the Expert

Walid Awad is Manager, Governance, Risk Management & Controls for SNC-Lavalin