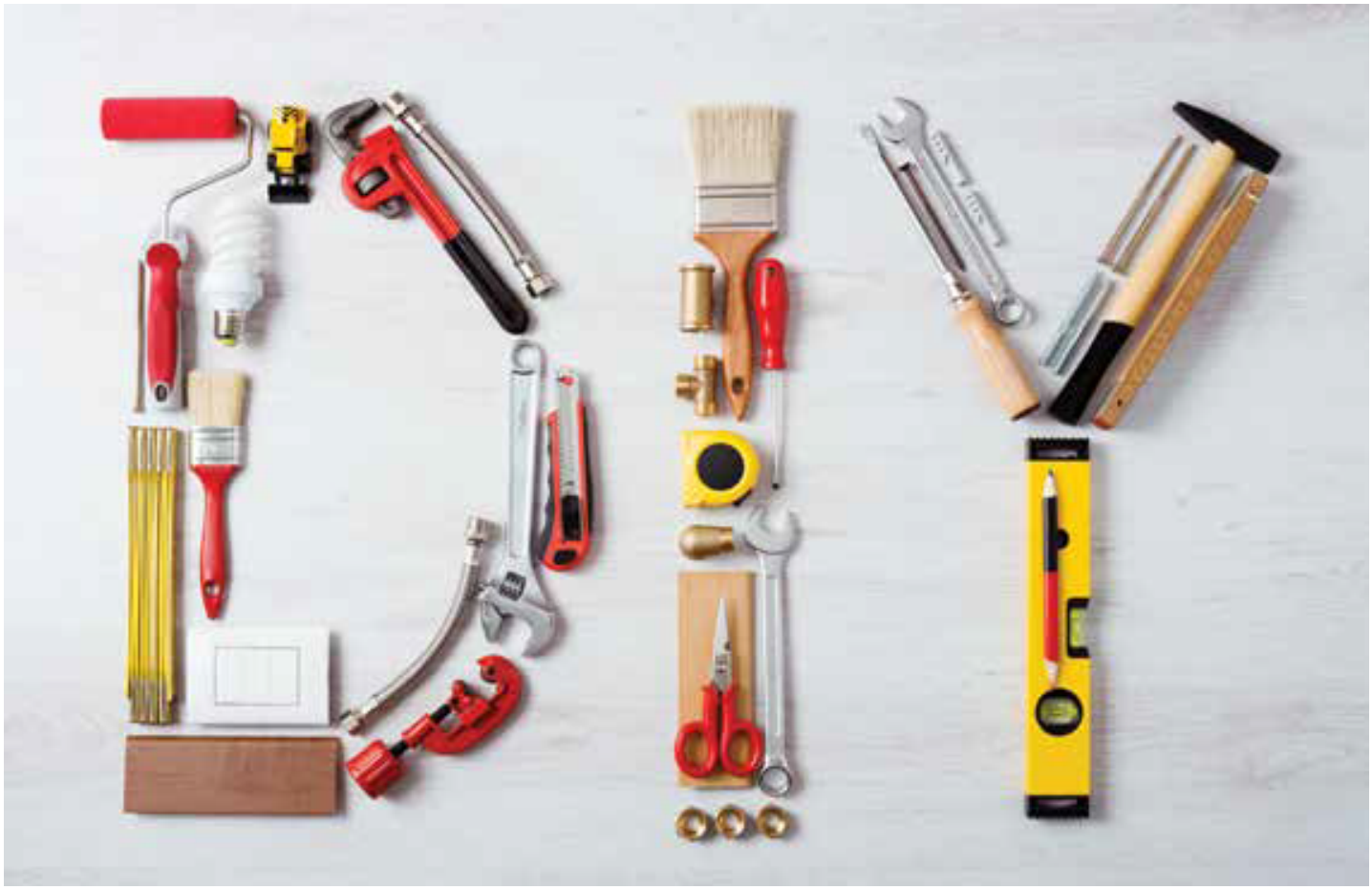
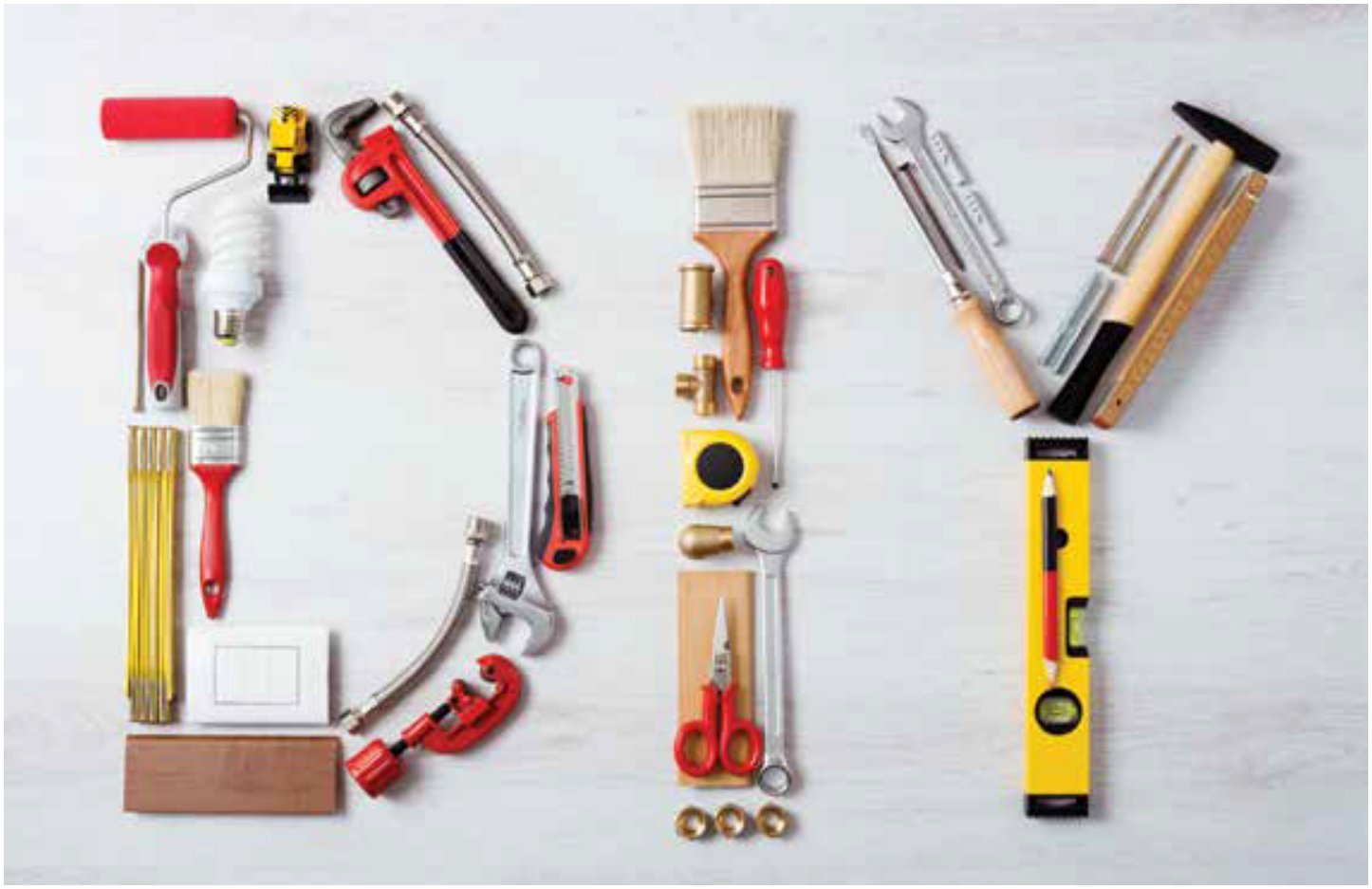
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

DIY Compliance Tools

Compliance and Ethics





In keeping with this month's Docket theme, this column focuses on some homegrown tools you could use to assist in your company's compliance efforts.[1]

Although there are many compliance-related tools out there, there are three basic categories of tools that most compliance professionals would agree are useful: an incident[2] reporting register database; a risk assessment register database; and a compliance dashboard to help senior management understand their company's compliance profile at a glance. Many vendors sell tools that do one or more of these things, but they are often more expensive and elaborate than necessary. A lawyer or other compliance professional may be able to build their own tools to serve most of their compliance needs.

I am going to focus on the first two, the incident reporting and risk assessment registers. Notice that although I characterized them as databases, I am using the term in the simplest sense to mean "a collection of information organized to provide efficient retrieval." So, although it might be best if you were able to create these in MS Access, Oracle, or some other Structured Query Language (SQL) based program, they would also work if you just made them in a simple spreadsheet program of your choice.

1 In case you are wondering about my compliance credentials, I was formerly the chief compliance officer for ACE NA and later the global compliance counsel for Chubb.

2 Note that, like many compliance professionals, I prefer the term "incident" to violation or breach, because (a) you don't want to jump to the conclusion that every reported incident necessarily

involves a violation, and (b) most registers are not likely protected from discovery, and you don't want to automatically create an admission against interest.

Incident reporting registers

All companies should have an incident reporting register. Regulators have started to expect them, and they help reinforce compliance initiatives. Plus, they are not that hard to create.

Many people use one tool or document for submitting an incident report and then a separate register that captures the salient details of those reports. Of course, how you go about this depends on your company's goals, complexity, compliance program, and risk profile but, if possible, I recommend keeping things simple by combining the two. Here are some of the elements you might put in a reporting spreadsheet or database program:

- Date of incident
- Date of report (if different)
- Reporting individual
- Type of incident (preferably in drop-down or other checklist selection format)
- The designated RACI (responsible, accountable, consulted, and informed) personnel
- Description of the incident
- Your mitigation plan, including milestones and timelines
- Status update
- Date closed

It's usually best if you house the register on your intranet, but you need to consider who needs and will have access to what. For example, if you have sufficient compliance personnel who can always serve as the reporting persons, you will better ensure consistency and care in the language used to describe the incidents.

Remember that the register may be tough to protect from discovery in litigation (and nearly impossible to protect from regulators), so your staff needs to be instructed on how to describe any incidents that arise. You will also need to provide clear guidance on things like escalation, which and when lawyers need to be involved, and when to consider involving communications or IT, etc.

Compliance risk assessment registers

Risk assessment is important. Companies that don't have a disciplined and systematic risk assessment process will always be fighting fires instead of preventing them. And they may not become aware of the fires until they've burned out of control. Any company trying to take advantage of good enterprise risk management techniques needs to make sure they take compliance risk into account.

But if you are new at compliance risk assessment, you may be wondering where to begin.

It's not actually that complicated. The first step is to develop a reasonably good risk catalog that lists and describes all the material compliance risks facing your company. Start by reviewing any incident reports and hotline or complaint logs, interviewing front-line personnel, and then assembling a team of experienced representatives from all the disciplines in your company that have compliance touchpoints (these days, that will be most of them): legal, compliance, marketing and sales, finance,

IT, etc. Use logic trees, mindmapping, or other brainstorming techniques to come up with a good list of compliance risks. Then ask your disciplinary experts to work with the legal and compliance department to develop satisfactory descriptions of your risks.

Now that you have a good risk catalog, you need to develop a pre- and post-mitigation risk scoring system. I recommend using a 1-5 scale with a two-factor system based on likelihood and severity, where 5 is the most likely and the most severe, and then using the product of those factors to represent the compliance risk.

For example, you may identify OFAC violations as one of your compliance risks and decide that the likelihood of a violation occurring as a result of your sales or other activities is only a 2, but the severity if one occurs is a 4. Then the pre-mitigation risk score would be an 8. Under this system, once you score all of your risks, the highest scores will represent the highest risks.

Next, you will need to work with your risk assessment teams to develop and describe your mitigation plans. Once you've done that to your satisfaction, perform a post-mitigation scoring to decide whether you have sufficiently mitigated your highest risks. Note how useful this can be — if your mitigation plans were too limited by budget or human resource complaints, you may be able to use the risk assessment itself to convince management to provide additional resources. Try to take advantage of formal project planning methodology to perform the actual mitigation and keep them on track and on budget.

In both the incident reporting and risk assessment registers, as in all other legal matters, the devil is in the details. But starting to create these things is certainly going to be illuminating and a step in the right direction. If you do a good job creating these, in either a spreadsheet or database format, you can use them to feed a dashboard to help your compliance professionals and senior management get a better grip on your company's risk profile. Compliance is critical.

Greg Stern

Former Global Integration Counsel

Chubb, Independent Consultant