Calculating the Cost of Compliance and Risk

The average cost of compliance came in at $5.47 million, while the average cost of noncompliance was $14.82 million. In fact, the average cost of noncompliance has risen more than 45% over the past ten years

(SumTotalSystems.com)

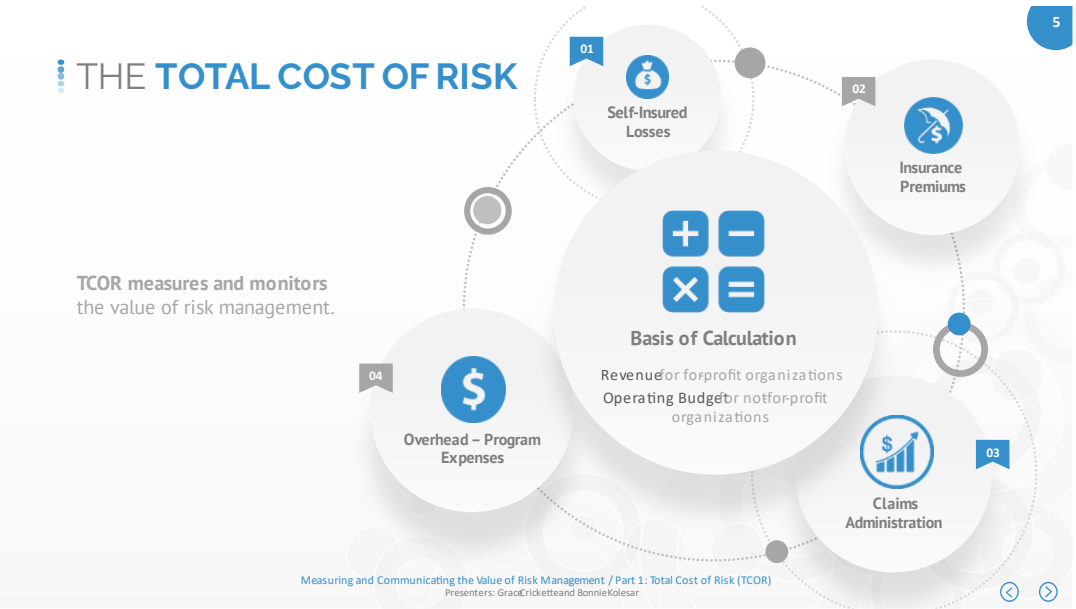
Examples of compliance risks:

- **Business Disruption |** When found to be noncompliant, we are often forced to implement compliance changes before we can resume. And if new processes need to be introduced to ensure compliance, further disruption can occur while these are implemented.
- **Possible Data Breaches |** Data protection regulations are increasingly complex due to personal and proprietary data's value and sensitivity. Noncompliance may increase the risk of data breaches, data loss, cyberattacks, or insider threats.
- **Reputational Damage |** This is one of the most overlooked costs of noncompliance. Repairing a damaged reputation is a difficult feat and often hard to accomplish in a timely fashion. Often manifests in increasing challenges with recruiting faculty and staff and recruiting and retention of students.
- **International Operations |** The complexity of global compliance is significant.
- **Revenue Loss |** Regulatory violations significantly impact our finances.
- **Other?**

Action Item | *How can we develop and collect examples of cost impact and cost of non-compliance and risk?*

One approach is to use the Total Cost of Risk (TCOR) methodology and customize it to include compliance and audit data (TCORCA)?

Calculating the Cost of Compliance and Risk



The total cost of risk is one of the most commonly used methods to measure and monitor the value of risk management, and it shouldn't be thought of as something that is exclusive to Enterprise Risk Management and can apply to the cost or savings from compliance programs or other areas that manage risk and controls.

The standard framework for a Total Cost of Risk report includes self-insured losses, premiums, claims administration, and loss control and loss prevention expenses as a percentage of revenue or operating budget. For the purposes of comparing by year, the total cost can be stated as an amount per $1,000 of revenue in a for-profit organization and more commonly in a government entity as $1,000 of operating budget for government entities. This standard framework can be prepared with or without an actuary.

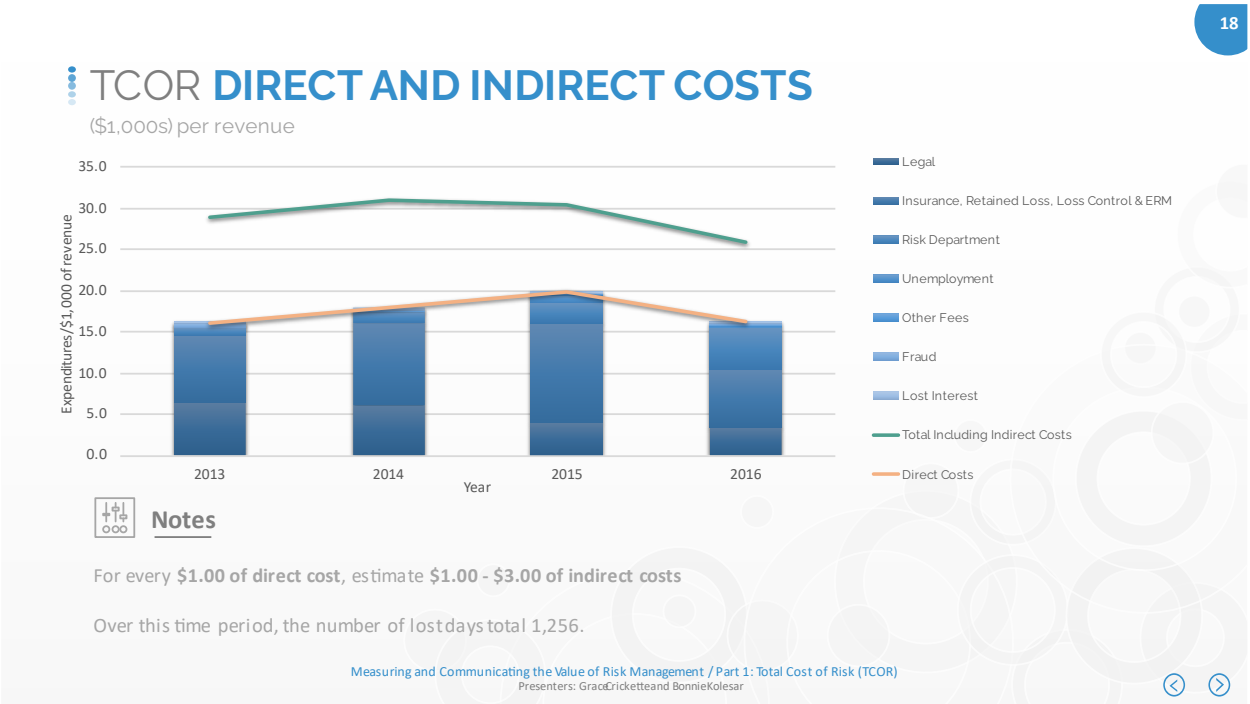
Some of you may find this information easily for your own organization, for example, data may be with UWSA or another department in your institution, or a public record.

TCOR Indirect Costs

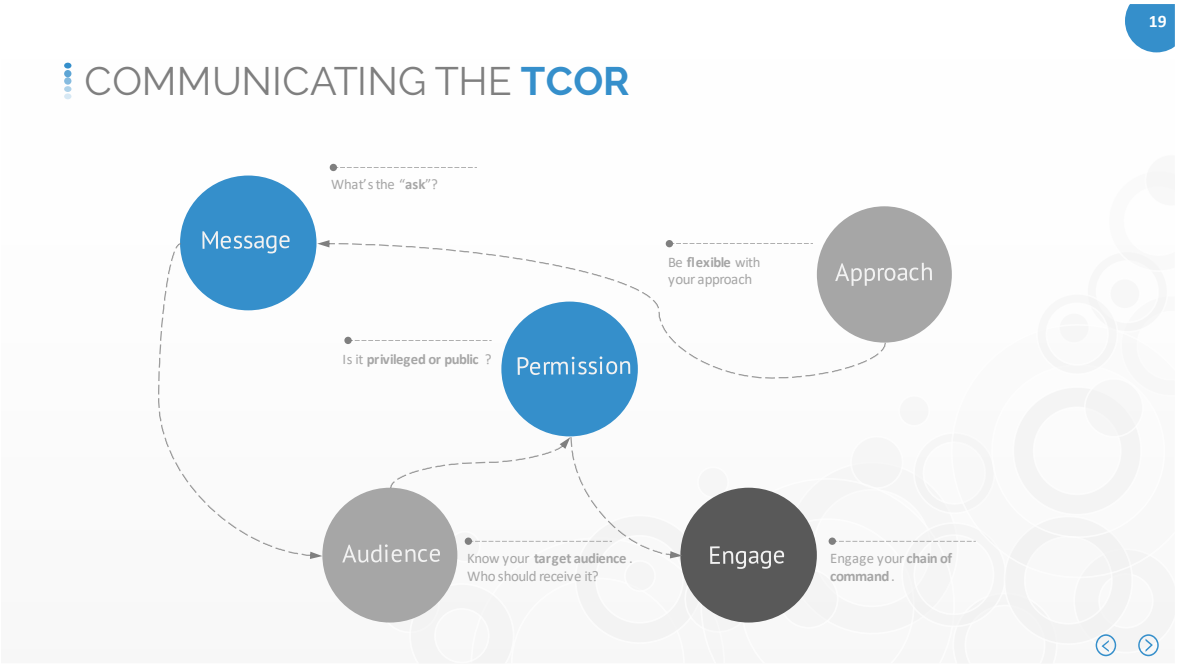
While hard costs (again, “direct” costs) are sometimes the first thing senior management pays attention to, soft or indirect costs can be even more significant. In fact, soft costs can be crippling to an organization. For example, when someone is out for extended periods of time due to injury or illness, audit response, responding to public records requests, attending legal and regulatory hearings, the organization feels it, too.

The lost workdays, lower productivity, and cost of hiring replacements are all indirect costs and they mount up quickly. Similarly, loss consulting services related to compliance and risk events require employee oversight and involvement to be effective. Based upon conservative actuarial estimates we have seen over the years, indirect costs in relation to direct costs is a 1 to 1 ratio, meaning that there is $1 of indirect cost for every $1 of direct cost. Estimates for some risks can range as high as a 3 to 1 ratio (source: Bickmore Actuarial Services).

Calculating the Cost of Compliance and Risk



So, how do we depict direct and indirect costs graphically? Here's an example using an assumption of a 1:1 ratio. In this chart, we have assumed no indirect costs associated with Risk Department, Loss Control & ERM Services, and Lost Interest expenses. These are the ACTUAL costs, or the total picture, an organization should be aware of in order to properly prioritize the risk severity.



Communicating the cost of risk and compliance is probably the most challenging professional risk you will face – and depending upon your organization, your role, the hierarchy, and even the culture, and you may have to adjust your approach. Really think about the message you're conveying – what's the "ask"? Or, simply stated: What's the point? If you share this, what are you trying to achieve? Who is your target audience (or Who will likely want to know)?

We want to see the core traditional risks represented and richer information over time. We also want to see other factors that are meaningful, and they will vary depending on the organization; also, a correlation of the changes over time that have impacted the bottom line. And then peripherally, we are always interested in seeing a heightened awareness created for such things as reputational loss, revenue donations, fraud, lost interest, and reputational impact. More importantly, what are we doing about it – what's the story behind it?

Action Item |What data/information would you want to include in calculating the cost of non-compliance, risk events, and audit findings?

Brainstorm with your team on identifying as many ideas as possible:

Retained losses (deductibles)

Insurance premiums

Hours spend responding to audits

Calculating the Cost of Compliance and Risk

Penalties (OSHA, late fines, interest payment)