



Thinking about the Most Serious Cases Reported by Organizational Ombuds

Mary Rowe PhD, Timothy Hedeem PhD & Jennifer Schneider PhD

Why keep data about the most serious cases?

Savings in costs and organizational reputation in *any* high-risk case—if it is handled quickly and effectively—may more than offset all the costs of an ombuds office. This benefit-to-cost ratio of the Organizational Ombuds (OO) is sometimes very apparent. For example, the value of the OO may be obvious after the OO identifies and helps to assess a serious issue, and finds an effective way to get relevant information to senior officers in a manner consonant with the IOA Standards of Practice. Sometimes in the first years of an OO office, its value is immediately apparent if the costs of serious issues are suddenly reduced, if important good ideas flow more freely, and systemic improvements happen more easily.

What are the most serious issues reported by OOs?

Insider threats, national security issues, sexual and racial harassment and bullying, waste, fraud and abuse, safety issues, potential suicidal and homicidal behavior, research and financial misconduct, retaliation and a variety of other integrity concerns are reported by most OOs. Most of these are rare concerns. However, allegations of sexual and racist harassment, bullying, safety, and retaliation are among the most *frequent* of all issues reported by OOs, (along with concerns about supervisor and managerial skills, suggestions for organizational improvement, and workload/overload.)

Ombuds also reported more *complex* cases.

They have been seeing more cases with: multiple issues, more multi-race-and-ethnic concerns, complex gender issues, multi-generational concerns, cases across units, cases involving conflicting rules, cases that took a long time, more cases with groups, more cases with bystanders. Many also reported more cases that became the impetus for focused or wide systemic responses.

From whom did OOs first hear about their most serious cases in the 2020 survey?

We asked ombuds to consider their five most serious cases and to check all the “first sources of information” that applied to those five cases. This question is important because it indicates a breadth of outreach and trust in the OO office.

Hearing first from the *complainant* was reported by almost nine-tenths, for at least one case. Hearing first from a *peer or bystander* was reported by nearly half the OOs, for at least one case. Hearing first from a *senior officer* was reported by nearly two fifths of OOs, for at least one case, and hearing first from a *supervisor* by a quarter of OOs.



Counseling services and health care practitioners were also reported by a quarter of all OOs for at least one case. And “*someone outside the organization*” was mentioned by an eighth of ombuds for at least one case. Previous IOA surveys have also reported hearing first from *perpetrators, security or police, HR, EAP, and “others.”*

Many options were used to get information about these cases to management.

Data from the surveys indicate that many OOs have had to deal with one or more situations in recent years that they considered as an “*imminent risk of serious harm.*” Survey responses indicate that OOs are able to practice effectively, both within their conflict management and risk management systems *and* within the IOA Standards of Practice. With respect to at least one case of the five cases involving the most serious issues, OOs reported using many different options in 2020 to get information to appropriate recipient(s):

Nearly four fifths reported having received permission from a constituent to use or transmit information without identifying the source. An OO might find a way to convey information to the appropriate recipient while shielding the source and also avoiding having the ombuds become a party to the case. For example, as one option offered by an OO, a constituent might write a detailed anonymous letter of concern addressed to a top manager, double-seal it, and slip it under the OO’s door. The OO could then take the letter to the addressee, noting that the letter had not been opened or read by the ombuds.

Almost three quarters reported that they helped their constituent to act directly—to find and use an effective way to get the information to the right person. Examples include helping the constituent to assemble the needed information, talk with a line manager or compliance officer, use a hotline, send a detailed, anonymous letter from an unremarkable location, or join with other constituents in sending a factual letter about shared concerns.

Nearly two-thirds reported that they had received permission to use information from a constituent, identifying the source. Examples might include that the OO went to an appropriate manager, identifying—with permission—how he or she received the information.

Nearly half reported that they had found another specific way of communicating critical information—that had not been identified on the survey—to an appropriate recipient. As an example from an interview with an OO, after long discussion, the constituent chose the option of contacting a trusted former manager. The former manager in turn spoke off the record with an old friend currently in senior management. That senior officer in turn immediately looked into the situation while protecting the source.



About a quarter reported that they found an effective way for a compliance office to find the information for itself. As an example, the OO might use a specific kind of generic approach. In this approach, they alert the relevant compliance office, providing sufficient, but anonymous, information that would help compliance officers — unobtrusively and effectively — to look for and review certain kinds of information — for example, in an apparently routine safety inspection, security review, or financial audit or other “spot check.”

*Six percent reported that they had breached confidentiality in one or more very serious cases, presumably having found no other reasonable option. (In two percent of all responses—which may represent a third of the cases where the OO reported breaching confidentiality—the OOs reported that they were *required* to report the concern.) In these cases of breaching confidentiality, the OO may also have perceived an imminent risk. This could happen when the OO judges that the issue is an emergency, for example, a potential suicide, or homicide. In such a case, OOs might report to line or staff managers in a way that made the source identifiable.*

From analysis of the “most serious case” responses in the 2016, 2018 and 2020 surveys, and from numerous conversations with senior OOs, we learned that ombuds are in fact willing to breach confidentiality, in accordance with the IOA Standards of Practice for imminent risk of serious harm—in the rare cases where the OO judges that a situation warrants this action. However, the survey data also indicate that the ombuds who took the survey were almost always able to offer options to their constituents to get information where it was needed, without compromising the confidentiality of their constituents.