CATAP and AETAP Joint Guidelines for the Practice of Threat Assessment and Management

Version 1
March 2024

Legal Notice

The *CATAP and AETAP Joint Guidelines for the Practice of Threat Assessment and Management* (the "*Guidelines*") were developed jointly by a committee comprising representatives of the Canadian Association of Threat Assessment Professionals (CATAP) and the Association of European Threat Assessment Professionals (AETAP). The *Guidelines* received final approval from and were adopted by the CATAP Board of Directors and the AETAP Board of Directors in March 2024.

CATAP and AETAP are not-for-profit societies that seek to support and promote best practices in threat assessment and management. They are not bodies with the legal authority to license threat assessment and management professionals or regulate the practice of those professionals. In publishing the *Guidelines*, they are not undertaking to render services for or on behalf of any person or entity. They disclaim and make no warranty, expressed or implied, as to the accuracy or completeness of the *Guidelines* for the particular purpose or need of any person or entity. They do not undertake to guarantee the performance of any provider's professional services by virtue of reliance on the *Guidelines*.

CATAP and AETAP Joint Guidelines for the Practice of Threat Assessment and Management

1. Introduction

Threat assessment and management are services delivered by diverse professionals working in a wide range of settings whose responsibilities include[1] protecting people from the harmful effects of violence. The services are also referred to as *behavioural threat assessment and management* and *violence risk assessment and management*. Although some professionals draw distinctions between the terms, the differences are of limited practical importance and so we use the terms interchangeably herein.

The Canadian Association of Threat Assessment Professionals (CATAP) and the Association of European Threat Assessment Professionals (AETAP) are not-for-profit organizations that support and promote best practices in threat assessment and management in Canada and Europe, respectively. Members of CATAP and AETAP prepared the *CATAP and AETAP Joint Guidelines for the Practice of Threat Assessment and Management* (the "*Guidelines*") based on a review of the relevant scientific, professional, and legal literature for the purpose of promoting best practices with respect to violence risk assessment and management for the benefit of those directly involved in and affected by such activities, as well as for the benefit of the public. The *Guidelines* are aspirational in nature and intent. They recommend rather than require specific activities and conduct, and they aim to help professionals exercise good judgment rather than restrict or replace professional judgment. The *Guidelines* are also general. They are not exhaustive in scope and not applicable to all situations professionals may encounter in their practice. In particular, the *Guidelines* are not applicable to the conduct of administration, research and program evaluation, pedagogical activities, or legal consultation. The *Guidelines* are intended to supplement rather than supplant other relevant legal, professional, or ethical standards. Finally, the *Guidelines* are a living document and will be reviewed and updated considering important changes in the relevant scientific, professional, and legal literature.

2. Definitions

2.1 *Violence* is a plan, attempt, threat, or act by one or more persons that recklessly or deliberately causes fear of, potential, or actual physical harm or grave psychological harm to one or more other persons without lawful authority. Although the range of conduct that falls within this definition of violence is broad, by its very nature, it is likely to violate criminal, civil, human rights, employment, occupational health and safety, or other laws.

[1] Throughout the *Guidelines*, "include" means "include without limitation."

2.2 *Risk* is the effect of uncertainty on the achievement of objectives. The uncertainty stems from incompleteness or imprecision in language, knowledge, or information. The objectives may be strategic, tactical, logistical, or operational in nature. Risk is typically used to characterize negative outcomes that may vary in terms of nature, seriousness, imminence, frequency, duration, or likelihood.

2.3 *Threat assessment*, also known as *behavioural threat assessment* or *violence risk assessment*, is the process of gathering information about one or more people to understand their potential for violence.

2.4 *Threat management*, also known as *behavioural threat management or violence risk management*, is the process of developing plans to mitigate people's potential for violence and safeguard those who may be impacted by it.

2.5 *Persons of interest* are people whose violence risk is being assessed or managed.

2.6 *Potential victims* are people who may be the target of violence perpetrated by persons of interest.

2.7 *Threat assessment professionals* are people who deliver threat assessment and management services to persons of interest or potential victims.

3. Orienting Guidelines

3.1 **Threat assessment professionals strive to respect and achieve the ultimate goal of threat assessment and management, which is to prevent violence or minimize the impact of violence on potential victims.** They recognize the intrinsic link between assessment and management, such that assessment in the absence of management and management in the absence of assessment are of little or no value. To this end, *inter alia*, they assist in identifying, implementing, and evaluating interventions that are both feasible and likely to be effective in each case.

3.2 **Threat assessment professionals strive to achieve and maintain a high level of competence.** To this end, *inter alia*, they familiarize themselves with relevant, up-to-date literature regarding the various forms of violence with which they work or are likely to encounter. Such literature includes books, chapters, journal articles, and other documents relevant to the nature of, causes of, risk factors for, and management of various forms of violence. They are also committed to ongoing professional development, self-reflection, and regular peer supervision, and aim to conduct their work within multi-disciplinary collaborations whenever possible.

3.3 **Threat assessment professionals strive to be aware of and compliant with the laws, policies, standards, and other documents that guide or are relevant to their work.** To this end, *inter alia*, they familiarize themselves with existing laws, policies, standards, and other documents, as well as any updates or changes to them over time.

3.4 **Threat assessment professionals strive to respect the basic legal rights and dignity of all persons involved in or affected by their work, including persons of interest and potential victims.** To this end, *inter alia*, they ensure that people who are asked to participate directly in the delivery of threat assessment and management services are informed of and are given the opportunity to exercise their constitutional, human, and privacy rights. They also ensure the services they deliver are appropriate and do not discriminate on the basis of gender, age, mental or physical disability, culture, language, ethnicity, religion, or other important group differences.

3.5 **Threat assessment professionals strive for fairness and impartiality in their work.** To this end, *inter alia*, they seek to minimize potential bias and maximize transparency and accountability, as relevant and appropriate. Steps to minimize potential bias include monitoring their own values, perceptions, and reactions, as well as avoiding conflicts of interest or multiple relationships with respect to, or advocacy on behalf of, people involved in or affected by their work. In the face of potential bias, they refuse to undertake work, recuse themselves from work in progress, or seek peer consultation concerning other steps to mitigate potential bias. Steps to maximize transparency and accountability include providing complete, accurate, and prompt information to people involved in or affected by their work, as relevant and appropriate.

3.6 **Threat assessment professionals strive to deliver threat assessment and management services that are individualized.** To this end, *inter alia*, they familiarize themselves with and consider the totality of relevant circumstances in each case, where relevant and appropriate, regardless of any specific procedures they use. Such circumstances include the behaviour, personal characteristics, lifestyle, and plans or intentions for the future of both persons of interest and potential victims. They consider not just people's problems, difficulties, or challenges, but also their strengths and resources.

4. Procedural Guidelines

4.1 **Threat assessment professionals strive to gather and integrate all the information that is reasonably necessary to do their work.** To this end, *inter alia*, they identify the information that is reasonably necessary and then attempt to gather it. They gather information from diverse sources, including interviews, observations, official records, and other documents. They use or rely on specialized information-gathering techniques (e.g., open-source information searches, covert surveillance), where relevant and appropriate. They attempt to corroborate critical information. They acknowledge in their communications when critical information they would have otherwise relied on was unavailable, incomplete, or outdated.

4.1.1 Threat assessment professionals do not rely solely on indirect information; wherever possible they gather information about persons of interest directly via interview or observation unless doing so would be inappropriate, unfeasible, or unsafe.

4.1.2 Threat assessment professionals do not rely on a single source of information in their work and do not rely solely on uncorroborated statements.

4.1.3 Threat assessment professionals do not rely on information that is or is likely to be outdated unless gathering updated information would be inappropriate, unfeasible, or unsafe.

4.2 **Threat assessment professionals strive to be alert for signs that persons of interest or potential victims may have physical or mental health problems and take appropriate action when such signs are apparent.** To this end, *inter alia*, they gather information about potential health problems, document and communicate any signs of potential health problems that come to their attention or undertake or recommend specialized assessment or treatment of health problems, as relevant and appropriate. They take care to respect the dignity of people with health problems and to avoid infringing on their legal rights. They carefully consider the extent to which health problems may affect the risks posed by persons of interest or the management of those risks.

4.2.1 Threat assessment professionals do not assume themselves or encourage others to assume that the mere presence of mental health problems means they are relevant to risk.

4.2.2 Threat assessment professionals do not assess or treat physical or mental health problems unless legally qualified to do so and unless they can do so in a way that maintains fairness and impartiality and avoids multiple relationships.

4.3 **Threat assessment professionals strive to identify and use structured evaluative devices or procedures.** To this end, *inter alia*, they acknowledge the limitations of unaided or unstructured professional judgment, seek education and training about structured evaluative devices or procedures germane to their work, and use structured evaluative devices and procedures where relevant and appropriate. They use structured evaluative devices and procedures only as recommended by authorities in the field, such as the developers. They acknowledge in their communications the strengths and limitations of any structured evaluative devices or procedures they used.

4.3.1 Threat assessment professionals do not rely solely on unaided or unstructured professional judgment when structured evaluative devices or procedures germane to their work exist and could be appropriately used.

4.3.2 Threat assessment professionals do not use structured evaluative devices or procedures unless adequately trained and experienced in their application, administration, and interpretation.

4.3.3 Threat assessment professionals do not use structured evaluative devices or procedures unless familiar with the professional literature regarding their reliability (precision) and validity (accuracy).

4.3.4 Threat assessment professionals do not use structured evaluative devices or procedures that are quantitative (i.e., rely on algorithms, statistical profiles, interpretive norms, or cutoff scores) or automated (i.e., rely on artificial intelligence

or other software) without clarifying in any oral or written communications which procedures they used or without providing an individualized and contextualized interpretation or explanation of findings based on those procedures.

4.4 **Threat assessment professionals strive to develop comprehensive management plans**. To this end, *inter alia*, they develop plans that identify potentially effective management strategies, tactics, and logistics. They ensure that plans target all important risk factors, but only important risk factors. They recognize the need for and facilitate coordination among the various professionals responsible for threat management, where relevant and appropriate. They acknowledge in their communications the need to evaluate and revise plans.

4.4.1 Threat assessment professionals do not deliver threat management services without adequate training and experience in those specific services.

4.4.2 Threat assessment professionals do not deliver threat management services without involving and collaborating with allied professionals, as relevant and appropriate.

4.4.3 Threat assessment professionals do not deliver threat management services without making contingency plans for continuity of service delivery in the event they are unable to work.

4.4.4 Threat assessment professionals do not neglect their legal obligations to protect the privacy or confidentiality of information they have gathered or disclose private information when necessary to protect people's health and safety.

4.5 **Threat assessment professionals strive to communicate with others about their work in a manner that is complete, accurate, and clear.** To this end, *inter alia*, they include in their oral or written communications all the information necessary, but only the information necessary, to describe their actions, findings, or opinions. They use non-technical language when communicating with people who are not threat assessment professionals, as relevant and appropriate. They acknowledge the limitations of their work.

4.5.1 Threat assessment professionals do not misrepresent or distort information included in their communications.

4.5.2 Threat assessment professionals do not ignore or omit potentially relevant information from their communications.

4.5.3 Threat assessment professionals do not use jargon in their communications unless necessary and unless they provide adequate definitions or explanations.

4.5.4 Threat assessment professionals do not present their findings or opinions without qualifying them considering limitations in the information on which they were based.

4.5.5 Threat assessment professionals do not present their findings or opinions without qualifying them considering the contextual and dynamic nature of risk.