← BACK TO

Guide - Introduction to SAFETAG

The Security Auditing Framework and Evaluation Template for Advocacy Groups (SAFETAG) is a professional audit framework that adapts traditional penetration testing and risk assessment methodologies to be relevant to small and medium, non-profit, human rights organizations based or operating in the developing world, taking into account the capacity constraints and unique threats faced in this community.

SAFETAG uses assessment activities derived from standards in the security auditing world and best-practices for working with small scale at-risk organizations to provide organization-driven risk assessment and mitigation consultation. SAFETAG auditors lead an organizational risk modelling process that helps staff and leadership take an institutional lens on their digital security problems, conduct a targeted digital security audit to expose vulnerabilities that impact the vital processes and assets identified, and provide post-audit reporting and follow-up that helps the organization and staff identify the training and technical support that they need to address needs identified in the audit.

info@safetag.org | https://safetag.org

The SAFETAG Audit Framework Core

The SAFETAG audit consists of multiple information gathering and confirmations steps as well as research and capacity-building exercises with staff. These are organized in a collection of objectives, each of which supports the core goals of SAFETAG: creating an information security risk assessment while simultaneously building the capacity of the organization to manage its risk.

These objectives provide collections of approaches and activities to gather and verify information in both technical and interactive/social methods and to assess and build capacity. Many of these activities include targeted exercises and walk-through instructions.

These are not meant to be a "checklist" or even a prescribed set of actions -- indeed, experienced auditors will deviate strongly from many of the specific activities. SAFETAG provides only a library of activities which auditors can draw from, as well as guidance on what a "minimal set" of audit activities would entail.

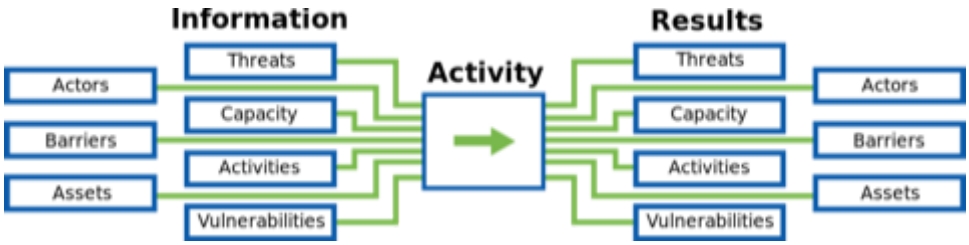
Indeed, many objectives and their specific exercises overlap or can be done together -- on-site interviews with staff can coincide with assessing their devices and keeping one's eyes open for physical security issues. Conversely, the data assessment exercises may provide enough information that other staff engagements are unnecessary.

The Life Cycle of an Audit

SAFETAG consists of a collection of high-level Methodologies, each with a variety of linked activities, that contribute towards the goals and their required information needs is represented here. Activites tend to fall in three broad approaches: Technical, Research, and Interpersonal. It is tempting to focus on the style of approach you as the auditor are most comfortable with - people with backgrounds in digital security training tend towards the interpersonal, people with pentesting backgrounds the technical. However, by using a combination of these, you get a clearer understanding of not only the organization’s setup and infrastructure, but how decisions are made, how policies are enforced (or not), and where there are opportunities for organizational change. Experienced Auditors will likely come up with their own approaches, and the SAFETAG project welcomes such contributions.

The audit process is very cyclical. Assessment activities reveal new threats, vulnerabilities, capabilities, and barriers which in turn shed new light on activities that have already been and have yet to be run. At the same time the auditor, through conversations, training, and group activities is actively building the organization's agency and addressing time-sensitive or critical threats insofar as possible within the time frame. This iterative process eventually leads to a point where the auditor is confident they have identified the critical and low-hanging fruit, and is confident the organization is capable of moving forward with their recommendations.

Each objective requires a certain base of information, and outputs more information into this cyclical process. Each objective has a "map" of the data flow that it and its specific activities provide:



- **Actors** are the people connected to an organization including an organization's staff, board members, contractors, and partners. Actors could also include volunteers, members of a

broader community of practice, and even the family members of principle actors. Actors also include potential adversaries of the organization such as competing groups.

- **Activities** are the actions and processes of an organization. While most NGO work revolves around program-based concepts, activities also include things like payroll.
- **Capacity** includes staff skills and a wide variety of resources that an organization can draw from to affect change including funding, networks, and institutional processes and policies.
- **Barriers** are specific challenges an organization faces that might limit or block its capacity.
- **Assets** are most easily conceptualized as computer systems - laptops and servers, but also include both the data stored on them and can also be services like remote file storage, hosted websites, applications, webmail, and more. Offline drives, USB sticks, and even paper records containing sensitive information are also assets.
- **Vulnerabilities** are specific flaws or attributes of an asset susceptible to attack.
- **Threats** are specific, possible attacks or occurrences that could harm the organization.

If a bucket of oily rags is a **vulnerability**, a fire is the **threat**. **Mitigations** would be rules against leaving oily rags around as well as fire extinguishers, smoke detectors, remote backup policies, and evacuation planning. Note that some mitigations may be outside the **capacity** of an organization -- perhaps there is limited budget (a **barrier**) for one fire extinguisher or one smoke detector, but not both. **Vulnerability** can be reduced by implementing mitigating strategies for the assets at highest risk of combustion or smoke damage. The auditor will need to work with the organization to review **assets**, **activities**, and **actors** as well as a detailed review of the **threats** to determine the organization's response.

These components are defined in greater depth in the Risk Assessment and Agency Building sections to follow.