SAFETAG

A SECURITY AUDITING FRAMEWORK AND EVALUATION TEMPLATE FOR ADVOCACY GROUPS

Minimal Viable Audit

Introduction

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, non-profit, human rights organizations based or operating in the developing world.

SAFETAG is based upon a set of principles, activities, and best practices to allow digital security auditors to best support at-risk organizations by working with them to identify the risks they face, the next steps they need to take to address them, and guidance on how to seek out support in the future.

The Minimal Viable Audit is designed as the starting point for an assessment to be considered viable under the SAFETAG framework. It primarily focuses on identification of possible threats in and to the organization, its capacity to deal with them, data management and organizational device usuage. It is intended to be used where time for the assessment is very limited, and a starting point is needed to determine the status of the organization.

For a more comprehesive assessment, use of the full SAFETAG guide and other tools will be required.

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

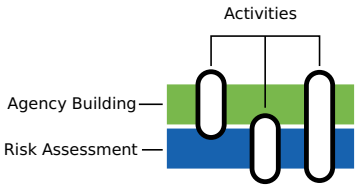
The SAFETAG Audit Framework

The SAFETAG audit consists of multiple information gathering and confirmations steps as well as research and capacity-building exercises with staff organized in a collection of objectives, each of which supports the core goals of SAFETAG, creating a risk assessment while also building the capacity of the organization.

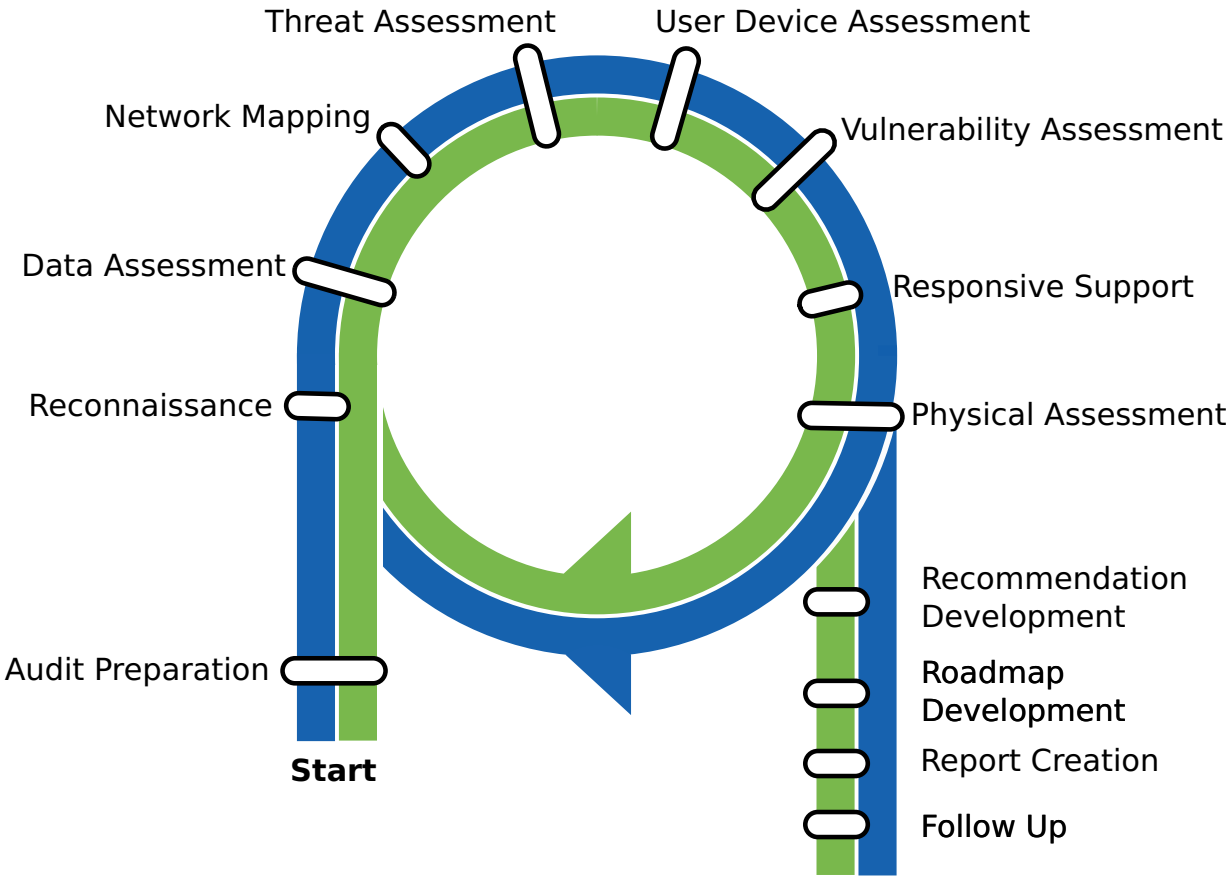
Audit Flow

SAFETAG

Activities Overview



Legend

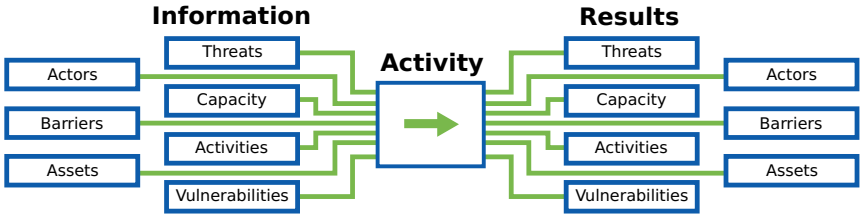


SAFETAG Activities

THE LIFE CYCLE OF AN AUDIT

The audit process in very cyclical. Newly identified threats, vulnerabilities, capabilities, and barriers impact activities that have and have yet to be run. At the same time the auditor, through conversations, training, and group activities is actively building the organizations agency and addressing time-sensitive or critical threats that are 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 based on this map:



SAFETAG Data Flow

While more completely defined below in the Risk Assessment and Agency Building sections, a brief overview of the data flow components:

- **Actors** Actors are the people connected to an organization include an organization's staff, board members, contractors and partners. Actors could also include volunteers, members of a broader community of practice, and even family members. Actors also include potential adversaries of the organization such as competing groups.
- **Activities** Activities are the actions and processes of an organization. While most NGO work revolves around mission-based concepts, activities also include things like payroll.
- **Capacity** Indicators of capacity include staff skills and a wide variety of resources that an organization can draw from to affect change.
- **Barriers** Barriers are specific challenges an organization faces that might limit or block its capacity.
- **Assets** 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, webmail, and more. Offline drives, USB sticks, and even paper printouts of relevant or sensitive information can also be included
- **Vulnerabilities** Vulnerabilities are specific flaws or attributes of an asset susceptible to attack.
- **Threats** A Threat is a specific, possible attack or occurrence that could harm the organization. If a bucket of oily rags is a vulnerability, a fire is the threat - and mitigations would be rules against leaving oily rags around as well as fire extinguishers, smoke detectors, remote backup policies, and evacuation planning.

To make SAFETAG approachable, a core evaluation template which links together a series of specific objectives, each with a variety of linked activities, that contribute towards the goals and their required information needs is represented here. Experienced Auditors will likely come up with their own approaches, and the SAFETAG project welcomes such contributions.

Audit Preparation

AGENCY BUILDING

SAFETAG differs from many risk assessment tools because it aims to build the host's and staff's capacity so that they are able to address the risks that the auditor has identified. SAFETAG is designed to provide in-audit activities and training that increase an organizations agency to seek out and address security challenges within their organization. To do this an auditor must collect information that allows them to identify organizational areas of strength and weakness (expertise, finance, willingness to learn, staff time, etc.)

A common refrain, among auditors, software developers and other specialists in this sector, is that digital security is not about technology; it is about people. This is undeniably true, and even the previous SAFETAG modules — despite their more direct fixation on technology — acknowledge this insight by emphasizing the educational and a persuasive roles played by your findings report.

Capacity

Definition: The combination of strengths, attributes and resources available within the organization that can be used to reduce the impact or likelihood of threats.

Example: This includes, but is not limited to technical skill, financial support, staff and management time, relationships, and legal power.

Barriers

Definition: The combination of weaknesses, assumptions, regulations, social or cultural practices, and obligations that get in the way of an organization implementing an effective digital security practice.

Example: Examples can include a lack of funding, lack of authority within an organization to mandate practices to their staff, resistance to change, high staff turnover, or digital illiteracy.

PREPARATION

SUMMARY

This component consists of trip preparation activities that are needed to ensure the technical and facilitated components of the audit are able to be conducted effectively and within the on-site time-frame and in coordination with the organization.

PURPOSE

A SAFETAG audit has a short time frame. Preparation is vital to ensure that time on the ground is not spent negotiating over the audit scope, updating the auditors systems, searching for missing hardware, or refreshing oneself with the SAFETAG framework. To that end negotiations with the host organization help reveal if the organization has the capacity to undertake the audit and respond to its findings.

GUIDING QUESTIONS

- Does the organization have existing digital security practice or attempted to implement them in the past?
- What is the process for procedure for incident handling in the event that auditor cause or uncover an incident during the course of the assessment?
- What are the legal, physical, or social risks for the auditor & organization associated with conducting the audit or having audit results leak? [1]
- Does the security situation of the location or organization require additional planning? Are your software tools up to date and working as expected?

APPROACH

- **Create an Assessment Plan:** Have a "scoping" meeting that outlines the level of access that an auditor will have, what is off limits, and the process for modifying the scope of the audit when new information arises. [2],[3]
- **Negotiate a Confidentiality Agreement:** Negotiate an agreement with the organization that outlines how an auditor will protect the privacy of the organization and the outcomes of the audit.
- **Establish an Emergency Contact:** Establish a procedure for incident handling and an emergency contact in the event that auditor cause or uncover an incident during the course of the assessment. [4],[5]
- **Prepare for Travel:** Check travel logistical needs -- visa, letter of invitation, travel tickets and hotel reservations. Note that some visas can take significant effort and may require the auditor to be without a passport while they are being processed.
- **Prepare Systems:** Update and test your systems, A/V and audit tools. [6], prepare storage devices and systems to reflect the required operational security, and ensure you have power supply adapters, cables and relevant adapters, usb drives, external wireless cards and any other equipment needed for testing. [7]^, [8]

OPERATIONAL SECURITY

"*Also be aware that local groups may not be able to accurately gauge the safety of their communications with you. Sometimes they underestimate the likelihood of risk - at other times, they can wildly overestimate the risk. Either way, trainers need to navigate this issues carefully and respectfully with a "do no harm" approach that respects the reported needs, context, and experiences of your local contact and potential trainees.*" - *Needs Assessment: Level-Up* [9]

SUMMARY

Below are the baseline operational security guidelines for a SAFETAG audit. Activity specific operational security guidelines are contained within each activity.

PURPOSE

An audit uncovers an array of sensitive information about an organization. For some at-risk populations the mere act of getting a digital security audit can increase their likelihood of being actively attacked by an adversary. The foundation of the SAFETAG process is the goal of increasing the safety of the host organization, its staff, and the auditor. It is vital that an auditor weigh the possible risk and audit may incur on the organization or the auditor against the possible outcomes of an audit.

OBJECTIVES

- Data storage security
  - Keep ALL data related to the audit secured per the Pentest Standards for data security, from interview and research notes through audit findings and reporting outputs. Additional notes per section.
- Communications security
  - Conduct all communication with the client over at least minimally secure channels where the communication is encrypted in transit at all times per the Pentest Standards for data security.
  - Higher levels of security (such as PGP, truecrypt, or minilock) should be used for all file and document transfers.

CONTEXT RESEARCH

SUMMARY

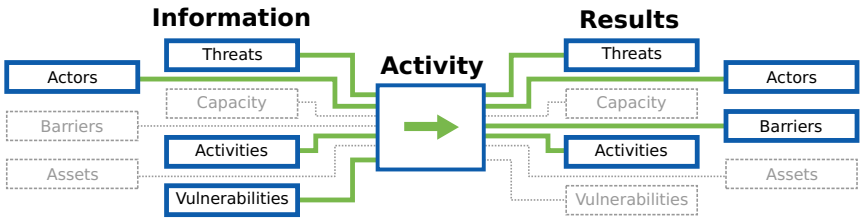
This component allows the auditor to identify the relevant regional and technological context needed to provide a safe and informed SAFETAG audit. This component consists of desk research that is collected and analyzed by the auditor, as well as inputs from the Interview component.

PURPOSE

Analysis of context is the foundation of effective risk management. Both at-risk organizations and auditors will develop assumptions based upon their experience. It is important that an audit is based on information that is current and accurate.

Checking the assumptions both of the organization and of the auditor by researching the current regional and technological context will ensure that an auditor is basing their work on accurate assessments of the conditions the organization faces and that they are making informed operational security considerations.

THE FLOW OF INFORMATION



Context Research Information Flow

GUIDING QUESTIONS

- What infrastructural barriers exist in the region?
- What are the top, non-targeted digital threats in this region?
- What are the top targeted digital threats facing organizations doing this work in this region / country?
- Are there legal ramifications to digital security in the country? (e.g. legality of encryption, anonymity tools, etc.)
- Has any organization or individual made specific threats, or demonstrated intention or mindset to attack on the organization or similar organizations?

APPROACHES

- RESEARCH: Search for background information that will help you better understand potential threats and overall context for the organization and the audit process.

Assessment and Analysis

RISK ASSESSMENT & ANALYSIS

Functionally, SAFETAG is a digital risk assessment framework. Risk assessment a systematic approach to identifying and assessing risks associated with hazards and human activities. SAFETAG focuses this approach on digital security risks. A SAFETAG audit will work to collect the following types of information in order to assess the risks an organization faces.

Risk is the current assessment of the possibility of harmful events occurring. Risk is assessed by comparing the threats an actor faces with their vulnerabilities, and their capacity to respond to or mitigate emergent threats.

The SAFETAG evaluation revolves around collecting enough information to identify and assess the various risks and an organization and its related actors face so that they can take action strategically.

$$\text{RISK} = \frac{\text{THREAT} \times \text{VULNERABILITY}}{\text{CAPACITY}}$$

The Risk Equation

PROGRAM ANALYSIS

Program analysis identifies the priority objectives of the organization and determine its capacities. This process exposes the activities, actors, and capacities of an organization.

Activities

Definition: The practices and interactions that the organization carries out in order to accomplish their goals.

Example: This includes any activity that the organization carries out to accomplish its goals and those that allow the organization to function (publishing, payment, fund-raising, outreach, interviewing.)

- What is the main purpose of the organization?
- What are the processes the organization takes part in to carry out their work?

Actors

Definition: The staff, volunteers, partners, beneficiaries, donors, and adversaries associated with the organization.

Example: The core organizational staff, the volunteers, maintenance, cleaning, security, or other non-critical staff, the partner organizations, the individuals and groups that the organization provides services to, groups of unorganized individuals who are opposed to organizational aims, governmental and non-governmental high-power agents and organizations that are opposed to the organizations aims.

- What staff does the organization have?
- Are their volunteers, maintenance, cleaning, security, or other non-critical staff who have access to the office?
- Who does the organization serve?
- Does the organization have any partners?
- Who are the organizations beneficiaries?

VULNERABILITY ANALYSIS

Understand the organisation’s exposure to threats, points of weakness and the ways in which the organisation may be affected.

Vulnerability

Definition: A attribute or feature that makes an entity, asset, system, or network susceptible to a given threat.

Example: This can include poorly built or unmaintained hardware, software, or offices as well as missing, ignored, or poor policies or practices around security.

THREAT ANALYSIS

Threat analysis is the process of identifying possible attackers and gathering background information about the capability of those attackers to threaten the organization. The basis of this information is a potential threats **history** of carrying out specific threats, their **capability** to carry out those threats currently, and proof that the threat has **intent** to leverage resources against the target.

Threat

Definition: A threat is a possible attack or occurrence that has the potential to harm life, information, operations, the environment, and/or property.

Example: Threats can range from *fire,* or *flood,* to *targeted malware, physical harassment,* or *phishing attacks.*

Threat History

Definition: What types of threats has the attacker used historically. And, what types of actors have been targeted by those threats.

Example:

- What history of attacks does the threat actor have?
- What techniques have they used? Have they targeted vulnerabilities that the organization currently has?
- Have they targeted similar organizations?
- What is known about the types of threats used by an threat actor to attack similar organizations?

Threat Capability

Definition: The means that the attacker has to carry out threats against the organization.

Example: This includes, but is not limited to technical skill, financial support, number of staff hours, and legal power.

- Does the threat actor have the means to exploit a vulnerability that the organization currently has?
- Does the threat actor have the means to leverage widespread threats against all similar organizations, or will they have to prioritize their targets?

Threat Intent

Definition: The level of desire for the attacker to carry out threats against the organization.

Example: Intent can be goals or outcomes that the adversary seeks; consequences the adversary seeks to avoid; and how strongly the adversary seeks to achieve those outcomes and/or avoid those consequences.

- Does the threat actor currently have the desire to conduct an attack against this type of organization?
- Is the organization a priority threat target for the threat actor?

PROCESS MAPPING AND RISK MODELING

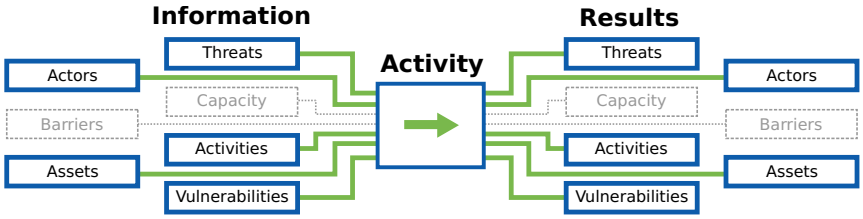
SUMMARY

This component allows an auditor to lead the host organization's staff in a series of activities to identify and prioritize the processes that are critical for the organization to carry out its work. These activities will also reveal the consequences if those critical processes were interrupted or exposed to a malicious actor. This results in the staff creating a risk matrix which is used as the foundation of the auditor's recommendations.

PURPOSE

Having the host organization central to the risk assessment process allows the auditor to put their threats and recommendations into the host's own narrative. With greater ownership of the process the staff will be more engaged in addressing the threats identified when the audit is complete. [10] By engaging as many staff as possible the auditor also is providing a framework for staff to examine future concerns when the auditor is gone. The existing in/formal security practices captured during this process will be used to remove organizational and psyco-social barriers to starting new practices.

THE FLOW OF INFORMATION



Risk Modeling Information Flow

GUIDING QUESTIONS

- What are the critical organizational activities?
- What threats does the organization, its programs, partners, and beneficiaries face?
- What would the impact of these threats be if they were to occur?
- What adversaries (people or groups) may attempt to carry out threats?
- Are those adversaries capable of carrying out these threats?

APPROACHES

- Process and/or data mapping exercises
- One-on-One interviews with staff to supplement other group activities.
- Risk identification based on process or data mappings
- A classic group Risk Assessment Activity.

Note: Risk modeling will require a mixed approach of exercises, and the order which you identify each component will vary depending upon the organization.

OUTPUTS

- Maps of critical processes.
- A list of organizational assets.

PROCESS MAPPING

Summary

This activity helps to identify the processes that allow the organization to function (publishing, payment, fund-raising, outreach, interviewing) the assets and systems (websites, software, PayPal) they rely on, and which ones are critical to their work. (Activity)

Participants are asked to "brain-storm" a list of all the processes that are critical for their work and the auditor works to map the details of critical processes out to expose points of risk.

Overview

- Brainstorm with staff all of the organizational processes
- Identify a smaller set which are mission critical
- Map the specific interactions and events that compose these processes to expose areas of risk

Materials Needed

- Stickies
- Markers
- Whiteboard or flip-chart

Considerations

- Treat device assessment data as well as any additional service information learned with the utmost security
- Ensure that any physical notes/drawings are erased and destroyed once digitally recorded.
- Ensure that any digital recordings of this process are kept secure and encrypted.
- Consider who has physical and visual access to the room where this process takes place, and if the room can be secured if this activity may span long/overnight breaks.

Walkthrough

The goal of this exercise is for the auditor to lead the host participants in "brain-storming" and mapping all the processes that are critical for the organization to carry out their work.

Additional Material

- Chart Paper or whiteboard.
- Marker pens or whiteboard markers.

GETTING STARTED

The auditor gives the participants a few example processes for a small independent media outlet.

- News gathering
- Editing
- Publishing
- User Feedback
- Lead Development
- Paying Staff
- Getting Advertisers
- Collecting Payment from Advertisers

Once the participants have brainstormed these out the facilitator leads the participants in identifying the critical processes (this may be all of the processes identified.)

- News gathering
- Editing
- Publishing
- Lead Development
- Paying Staff

The trainer then begins a free-hand process mapping activity for each process. You will be "charting the sequence of events of the work."

A Process Map shows

- The people involved; * The tasks, conversations, and decisions they carry out;
- The flow of materials, information and documents between them;
- The relationship and dependance between the steps.

CONDUCTING THE ACTIVITY

- **List all organizational processes:** The goal of this exercise is for the auditor to lead the host participants in "brain-storming" a list of all the processes the organization takes part in to carry out their work. It is important to remember this is a brainstorming session of all of the processes that occur in the organization.
    - Quickly identify the main purpose of the organization. If the organization is an online newspaper, the purpose then is to create, distribute, and diversify the content they are providing to their consumers.
    - Write out the list of all the processes that would occur in a very busy week at the office. This is a brainstorming session with your participants so it is important to get them to identify as many different processes at the beginning.
    - Once a complete list has been created, the auditor will then go through through to identify with the participants the critical processes within the organization – that is, without these processes the organization would not be able to function or function at a very poor level
- **Determine critical processes:** During this exercise the aim is for the auditor to lead the attendees in narrowing down the subset of activities to those that are crucial to their work.
    - step 1
    - step 2
    - step 3
    - step etc.

NOTE: If an auditor does not ensure that the uniquely identified subset of processes speaks to the full range of participants, their recommendations are more likely to be met with resistance.

- **Map out critical processes:** In this exercises the auditor does free-hand mapping for each process guided by the host participants. The auditor needs to make sure that they work to develop a broad understanding of the overall process. This is a time consuming activity, and managing their overall time to complete the entire needs assessment, and respect the time constraints of the staff, is critical.
    - Clearly identify the process name on the whiteboard or flipchart
    - Identify the first and last steps from the participants and write them on the side of the paper to keep the participants on track.
    - Place the "Starting" place on the white paper.
    - Have your participants explain to you what the process is step-by-step, while making a note on the side where there will be follow on processes.
    1. Don’t forget about follow-on processes
    2. List who does each step along side each process
    - Verbally walk the participants through the completed process so you ensure you didn’t miss anything
    - Take quick notes to remind yourself of any key points not clearly marked on the map before they move on to the next activity.

- After completing all the key events take a photo of the whiteboard / store the chart-paper for later documentation.

While doing this it is important to consider level of detail you will be mapping out (this should be pre-determined or established so everyone is on the same page)

How to make a process map

This process map will be used to develop our asset map.

"Draw the flowchart initially to represent the operation, as it actually happens - NOT what you might prefer it to be! Use a flip chart or whiteboard to produce your initial charts"

```
"WHO does WHAT (Job title/Function e.g. Level A1)
WHAT is done and WHEN
What DECISIONS have to be taken and
What possible paths follow from each decision"
```

Keep it simple to facilitate broad understanding of the OVERALL process. Too much detail early on can be overwhelming and/or lead to confusion. If you agree that more detail is required on a particular action, it is easy to highlight that box and produce a separate chart showing the process taking place within.

Recommendation

This activity can lead to feelings of hopelessness; it is important to remind the staff that any risk can be mitigated, and indeed it is the goal of an audit to identify the highest priority ones based on actual likelihood and provide guidance on mitigation.

THREAT ASSESSMENT

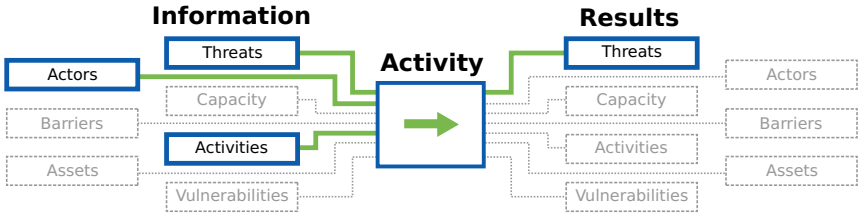
SUMMARY

This objective uses a variety of activities to identify possible attackers and gather background information about the capability of those attackers to threaten the organization. This consists of identifying a particular attacker's history of carrying out specific threats, their capability to carry out those threats currently, and proof that the threat has intent to leverage resources against the target.

PURPOSE

Checking the assumptions both of the organization and of the auditor by researching the current threats will ensure that an auditor is basing their work on accurate assessments of the conditions the organization faces and that they are making informed operational security considerations. With greater ownership of the process the staff provides an opportunity to explore their threat landscape and become more engaged in addressing the threats identified when the audit is complete. By engaging with as many staff as possible the auditor is providing a framework for staff to explore threat identification processes when the auditor is gone.

THE FLOW OF INFORMATION



Threat Assessment Information Flow

GUIDING QUESTIONS

- Who are potential adversaries for the organization?
- Do these threat actors have a history of attacks? Against whom?
- What types of organizations have they targeted?
- Does the threat actor have the means to leverage widespread threats against, or will they have to prioritize their targets? Is the organization a priority threat target?
- Do they have the desire and ability to conduct an attack?

APPROACHES

- **Open Source Threat Research:** Identify possible adversaries and threats using publicly available reports, news, and databases.
- **Threat Mapping:** Facilitate group activities where staff identify possible adversaries and the threats that they have/can leverage against the group.

OUTPUTS

- A host driven threat-matrix including the following:
  - **Adversaries** (threat actors) with capabilities and willingness
  - **Impacts** of attacks against **critical processes**, ranked by severity
  - **Likelihood** of each (based on adversaries)
- Latest general cyber-security threats
- Identify existing in/formal security practices that the participants use to address risks.

THREAT IDENTIFICATION

Summary

These activities build off of a process or data mapping exercise to connect actual processes or assets and data of the organization with potential threats, then drilling down into specific, likely threats the organization faces, adversaries who might take advantage of them, and the impact of this happening.

The goal is to be able to answer the following questions:

Threat History

- What history of attacks does the threat actor have?
- What techniques have they used? Have they targeted vulnerabilities that the organization currently has?
- What is known about the types of threats used by an threat actor to attack similar organizations?

Threat Capability

- Does the threat actor have the means to exploit a vulnerability that the organization currently has?
- Does the threat actor have the means to leverage widespread threats against all similar organizations, or will they have to prioritize their targets?

Threat Intent

- Have they targeted similar organizations?
- Does the threat actor currently have the desire to conduct an attack against this type of organization?
- Is the organization a priority threat target for the threat actor?

Overview

- Identify and categorize threats to processes or data (requires a process or data mapping exercise) by Confidentiality, Control, Integrity,

Identity, Availability, and Auditability
- Identify the impact of each threat against People, Organization, and Program
- Brainstorm potential Adversaries and note their History, Intent, and Capability per Threat
- For Threats with identified Adversaries, rank them on a linear scale from "Inconvenient" to "Severe" (no two items can have the same rank)

Materials Needed

- The outputs from a process or data mapping exercise to work from
- Stickies
- Whiteboard or flip-chart (whiteboard preferred)
- Markers
- Camera to digitally capture the data

Considerations

- Treat threat and adversary data with the utmost security.
- Ensure that any physical notes/drawings are erased and destroyed once digitally recorded.
- Ensure that any digital recordings of this process are kept secure and encrypted.
- Consider who has physical and visual access to the room where this process takes place, and if the room can be secured if this activity may span long/overnight breaks.

Walkthrough

- Requires a process or data mapping exercise's outputs

Threat Identification: (30 minutes per process)

- Give participants a "cheat sheet" of threats.
- Explain the types of threats.
  - **Confidentiality**: If unauthorized individuals find out an asset/process exists.
  - **Control**: If an asset/process can be accessed by unauthorized individuals.
  - **Integrity**: If an asset/process is changed without permission.
  - **Availability**: If an asset/process becomes unavailable.
  - **Consistency**: If an asset/process becomes unreliable. (Some use **Identity** instead or in addition to Consistency, if an asset/process can be spoofed to appear as owning/coming from someone else.)
  - **Auditability**: If you cannot verify that an asset/process is secure.
- Identify a "interaction line" from the process map to start with.
- Generate a list of threats that would cause that interaction to fail.
- Mark the back of the post it with the interaction name or number.
- Write the threat and their impact on post-its and arrange them in an orderly way.
- If multiple risks cause the same consequence create a new post-it near the new risk.
- Continue doing this for all the interactions in the critical process'.
- Discuss and rearrange threats as groupings emerge.

- Label threat clusters that appear.

- **NOTES:**
  - If any of the impacts identified in the pre-mortum or other process-mapping exercises are not covered ask participants where they would go.
  - Take photos of the threats once you have finished enumerating them.
  - Write risks on one set of post-its and impacts on another color of post-its to make it easy to keep track.
  - Look at the"CVSS V2 Base Metrics" for an example of the severity of different threats.

Impact Identification: (30 minutes per process) This exercise has the trainee lead the participants on a brainstorming of hypothetical consequences (impacts) when the threats identified earlier occur.

- Give participants a pen and three sticky note pads.
- Explain the topic and the categories. [11]
  - Staff/People - (which includes families, friends, and beneficiaries): temporary or permanent physical injury, temporary or longer-term psychological damage, death, legal costs, cost of medical treatment, loss of morale or trust in management.
  - Organization - loss of or damage to assets, operational inefficiency, loss of program quality or outright suspension; loss of reputation; loss of funding.
  - Program - reduced program quality, temporary suspension of the program, forced termination of the program.
- Instruct each person to generate DIRECT impacts based upon the exiting threat clustering from **Threat Identification.**
- Include only one impact per sticky note.
- Have one participant quickly describe then place an impact on the board writing along side it the threat that causes it.
- Invite others to place similar/the same impacts in proximity and quickly describe how it can occurs.
- Repeat the process until all impacts are included.
- Have participants add stickies for any secondary/cascading impacts
- Discuss and rearrange impacts as groupings emerge.

- Label impact clusters that appear.

- **NOTES:**
  - Tell participants to write multiple impacts per color.
  - Look for opportunities to create sub-groups.
  - Limit the time frame for discussion.
  - Take photos of the impact clusters once you have finished enumerating them.

Adversary Exploration (Likelyhood):

- Explain the topic and the categories. [12]

- "History – a past incidence or pattern of attacks on similar organizations."
- "Intent – specific threats, a demonstrated intention or mindset to attack."
- "Capability – the wherewithal to carry out an attack."

- Brainstorm adversaries who have demonstrated likelihood to impact their work or one of the process'.
- Pick an adversary and write their name on the board.
- Write specific instances of adversary history, intent, and capacity announced by the participants.

- Repeat the process until all adversaries are completed.

- **NOTES:**
  - Limit the time frame for discussion.
  - Take photos of the adversary lists.

Impact Ranking: The goal of this exercise is to have the trainee lead the host organization in classifying the severity of the possible impacts from the threats they have just explored.

- Create a post it for each impact.
- Place two points on the wall. On one side are "Inconvenient" impacts that disrupt the organization in a very small way. On the other side are "critical" impacts that may pose life-safety risks to employees, partners, or the general public.
- The low end of the scale may include a fire alarm may cause the staff to lose a half an hour of work time, but does not impact any short or long-term activities.
- The high end of the scale would include events such as a fire that destroys the organizations headquarters and endangers staffs lives or legal issues that cause termination of the program.
- Place each item along the severity line from least to most severe impact.

- Give each item its own place on the scale. No two items can be the same severity.

- **NOTES:**
  - Listen carefully to every point of deliberation.
  - As risks are placed on the wall, the trainee can use other already ranked risks to help participants identify the right place. "Is a robbery more or less likely than a fire?"
  - Take photos of the impact scale once you have finished it.

Recommendation

CALCULATIVE IMPACT IDENTIFICATION

Threat type	Impact	Likelihood	Risk
HUMAN THREATS			
1. Accidental destruction, modification, disclosure of confidential information			
2. Ignorance: inadequate security awareness, lack of security guidelines, lack of proper documentation, lack of knowledge			
3. Workload: Too many or too few system administrators, highly pressured users			
4. Users may inadvertently give information on security weaknesses to attackers			
5. Incorrect system configuration			
6. Inadequate security policy			
7. Dishonesty: Fraud, theft, selling of confidential information			
8. Attackers may use telephone to impersonate employees to persuade users/administrators to give user name/passwords, etc			
GENERAL THREATS			
1. Unauthorized use of “logged-in” computers			
2. Installation of unauthorized software or hardware			
3. Denial of service, due to Website traffic, large PING packets, etc.			
4. Malware in programs, documents, e-mail attachments, etc			
IDENTIFICATION AUTHORIZATION THREATS			
1. Attack software masquerading as normal programs (Trojan horses)			
2. Attack hardware masquerading as normal commercial hardware			
3. External attackers masquerading as valid users			
4. Internal attackers masquerading as valid users			
PRIVACY THREATS			
1. Telephone eavesdropping (via telephone bugs, inductive sensors, or service providers			
2. Electromagnetic eavesdropping			
3. Rubbish eavesdropping (analyzing waste for confidential documents, etc.)			
4. Planted bugs in the building			
INTEGRITY/ACCURACY THREATS			
1. Deliberate damage of information by external source			
2. Deliberate damage of information by internal sources			
3. Deliberate modification of information			
ACCESS CONTROL THREATS			
1. Password cracking (access to password files, use of default/weak passwords, etc)			
2. External access to password files, and sniffing of the networks			
3. Unsecured maintenance of online services, developer backdoors			
4. Bugs in network software which can open unknown/unexpected security holes (holes can be exploited from externally to gain access)			
5. Unauthorized physical access to system			

LEGAL THREATS			
1. Failure to comply with legal requirements			
2. Liability for acts of internal users or attackers who abuse the system to perpetrate unlawful acts (ie, incitement to racism, gambling, money laundering, distribution of pornographic or violent material)			
3. Liability for damages if an internal user attacks other sites			
RELIABILITY OF SERVICE THREATS			
1. Major natural disasters, fire, water, earthquake, floods, power outages, etc			
2. Minor natural disasters, of short duration, or causing little damage			
3. Equipment failure from defective hardware, cabling, or communications system.			
4 Denial of Service due to network abuse: Misuse of routing protocols to confuse and mislead systems			
5. Downloading of malicious Applets, Active X controls, macros, PostScript files, etc through the browsers			
6. Sabotage: Physical destruction of network interface devices, cables			

Risk = Impact * Likelihood

SCALE

Impact Scale	Likelihood
Impact is negligible =1	Unlikely to occur =0
Effect is minor, major organization operations are not affected=2	Likely to occur less than once per year =1
Organization operations are unavailable for a certain amount of time, costs are incurred. Public/customer confidence is minimally affected =3	Likely to occur once per year =2
Significant loss of operations, significant impact on public/customer confidence =4	likely to occur once per month =3
Effect is disastrous, systems are down for an extended period of time, rebuilding and replacement of systems is required =5	Likely to occur once per week =4
Effect is catastrophic, critical systems are completely down for an extended period; data is lost or irreparably corrupted; public and customers are totally affected =6	Likely to occur daily =5

CAPACITY ASSESSMENT

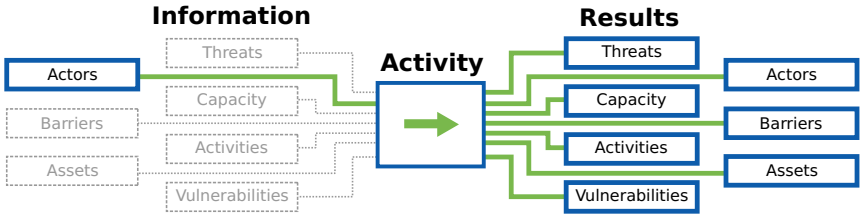
SUMMARY

In this component the auditor engages with staff through interviews and conversations to identify the organization's strengths and weakness (expertise, finance, willingness to learn, staff time, etc.) to adopting new digital and physical security practices. The auditor uses this information to modify the audit scope and recommendations accordingly.

PURPOSE

Knowing an organization's strengths and weaknesses allows the auditor to provide more tailored recommendations that an organization will be more likely to attempt and achieve. The auditor will use this assessment in preparing for the audit itself as well as when evaluating the difficulty of a recommendation. This information also provides a starting place for understanding the organization's current use and understanding of technology, digital security, and current threat landscape, as well as revealing elements of an organization's workflow, infrastructure and even vulnerabilities that you might otherwise have overlooked.

THE FLOW OF INFORMATION



Audit Preparation Information Flow

GUIDING QUESTIONS

- What is the organization's ability to adopt new technologies or practices?
- What resources does the organization have available to them?
- What is the environment that the organization works within like? What barriers, threat actors, and other aspects influence their work?
- Are there any specific considerations for the audit that would require modifying the overall approach, tools, preparation steps, or timeline?

APPROACHES

- Conduct pre-audit interviews with key managerial and technical staff to identify organizational areas of strength and weakness (expertise, finance, staff time, etc.).
- Have informal conversations with staff during the course of the audit to further gather capacity and historical "stories" of technology adoption.

OUTPUTS

- Organization's ability to:
  - Adopt new technology
  - Learn from others
- Organization's resources (financial, time, buy-in, expertise...) available for technological adoption
- The availability and quality of communications and electronic infrastructure.
- Threats posed to the digital and physical security of the organization and its staff, and past security issues encountered by the organization and its partners.
- Priority security concerns.
- Technological hardware and software in use for protecting the physical and digital security of organizations and their staff.
- Past, current, or desired use of websites, blogs, social media and other web-based tools and platforms to conduct outreach, manage information, advocate or engage with specific groups.
- Past, current, or desired use of mobile telephony and related software and hardware for activities such as sms management and data collection.

INTERVIEWS

Summary

The auditor conducts interviews with various staff members to gather information on the organizations risks and capacity.

Q&A sessions are unabashedly *white box* aspects of a security assessment, and you will occasionally hear push-back along the lines of, "You wouldn't have found that thing if we hadn't told you about this other thing." Compelling *black box* findings certainly do have an advantage when it comes to persuasiveness, but obtaining them can be quite time-consuming, so relying exclusively on vulnerabilities that you can identify without "help" is generally a mistake in this resource-constrained sector.

Overview

- Set up secure channels for communication
- Interview managerial staff
- Interview technical staff
- Use the Categories (at the end of the sample interview questions) to help scope which questions to ask
- Use the Capacity Assessment Cheat-Sheet to track topics you have covered

Materials Needed

Considerations

- If the auditor or organization believes that there is a good chance of surveillance on the channel you are communicating over, do the rest of the interview on a secured channel or in person where possible, though some information-gathering is critical to do before planning the audit. Inability to do so contributes towards a no-go situation.

Walkthrough

See the Appendix for a sample set of interview questions

CAPACITY ASSESSMENT CHECKLIST

Summary

A monolithic, one-time interview with key staff is not always possible or advisable, but interacting with a variety of staff exposes valuable information about every aspect of the audit, from vulnerabilities to capacity to hidden barriers. This serves as a "cheat sheet" of some topics to explore both during the planning and preparation phase and throughout the audit process.

Walkthrough

"Homework"

- Basic contact and organizational information: name, org, org's stated mission
- Contextual research

Organizational

- Size of staff
- Key roles in org for tech and management
- Structure: Management and Technical?
- (Program size, activities, information)
- (Change management)
- Languages used in office

Contextual / Background / Threat information

- What (if any) threats have occured to the organization and its partners? (digital, physical)
- Surveillance?
- What other threats are you concerned about? What has happened to other organizations in the space?
- Org responses to these threats - trainings, technical responses, organization process/change successes?
- Specific programs or other work outside of publicly stated mission that are high-risk
- Program use of technology (SMS surveys, blogs, facebook pages, other websites, media recording and broadcast ...?)

Technical:

- Primary website:
- Additional websites:
- Website technologies (content management, hosting provider)
- Technology in use:
- Desktop software (OS, Office)
- Desktop security tools (anti-virus, anti-malware, firewalls, vpns, disk encryption...)
- Servers (email, shared file system, networking tools, backups)
- Email, email hosts
- Other communication tools - skype, facebook, chat, mobile...
- Other less formal tools - external emails, dropbox...
- Internal network - wired, wireless, type of wireless network, ISP

Preparation Support

- Infrastructure
- How is the office connected to the Internet?
- Power outages or other challenges?
- Office setup and size
- Shared office space, shared floor or building?
- Physical security of the office?

DATA ASSESSMENT

SUMMARY

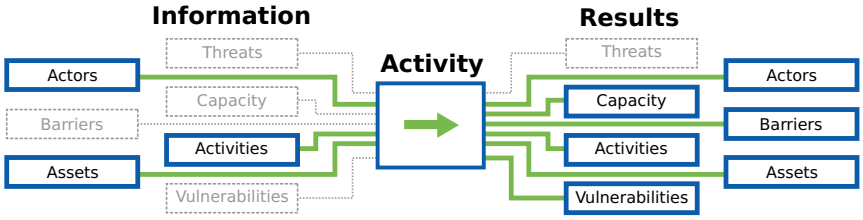
This component allows the auditor to identify what sensitive data exists for the organization, where it is stored, and how it is transferred.

PURPOSE

Sensitive files are often stored across multiple devices with different levels of security. A data assessment allows the auditor to recommend secure storage solutions which best meet the organizations risk assessment and workflow needs. While the auditor has insight on some of this based on the Network Access and Network Mapping work, cross-staff understanding and agreement on what constitutes sensitive data will support later organizational change.

An adversary who obtains a laptop, workstation, or backup drive will be able to read or modify sensitive information on the device, even if that staff member has set a strong account password. This applies to threats involving loss, theft, and confiscation, but also to "checkpoint" scenarios in which they may only have access for a few minutes. Furthermore, in the event of a burglary or office raid, an adversary could obtain all sensitive information on the organization's devices, possibly even undetected.

THE FLOW OF INFORMATION



Data Assessment Information Flow

GUIDING QUESTIONS

- What are the most important data sets to keep available? Are there backups?
- What are the most important data sets to keep private?
- How does the organization currently determine who should have access to data?
- Is there currently anyone who has access to data who should not?
- Does the staff agree on what constitutes sensitive data?
- What data does each staff member need to be able to access in order to do their job?

APPROACHES

- **Data Mapping Activity:** Have staff identify where that data is currently (what devices/physical locations), who has access (physical, login, permissions), and who needs to have access to get the organizations work completed.
- **Risks of Data Lost and Found Activity:** Have rank the impact if different data within the organization was lost, and if adversaries gained access to that data.
- **Private Data Activity:** Guide staff through an activity to have them list private data within the organization [13]

OUTPUTS

- A map of the staff's understanding of critical organizational data:
  - what that data is,
  - where it is stored,
  - who has access,
  - who needs access.

SENSITIVE DATA

Summary

Data and meta-data about an organization and its staff is incredibly difficult to keep track of over time, as people or projects use cloud services like Dropbox or Google Drive for some activities, a shared server for others, and a mix of work and personal devices (laptops, phones, tablets...).

This is natural, but it is important to keep track of where your organization's data lives and who can access it.

Overview

- With staff input, post up popular places where data is kept (laptops, email, shared drives...)
- Using stickies, gather from the staff what data is kept in what locations - duplicating notes when needed
- Rank data by sensitivity
- Discuss the impact of one of the devices where data is stored being lost - are there backups?
- Discuss the impact of a device being exposed / taken by an adversary
- Identify who has access (physical access, login access, and permissions), and who needs to have access to get the organizations work completed.

Materials Needed

- Stickies and markers for activities
- Flip chart paper or a whiteboard
- Camera to record outputs digitally

Considerations

- Some of the stickies generated in this activity may provide sensitive data, dispose of them responsibly.
- If you take photos for reporting needs, save the image files in a secure, encrypted container.

Walkthrough

Sensitive Data Assessment Activity

Duration: 45 minutes

This exercise is adapted from the LevelUp Activity, Backup Matrix, part of the curricula for Data Retrention and Backup by Daniel O'Clunaigh, Ali Ravi, Samir Nassar, and Carol.

Materials to Prepare:

- Stickies
- Markers
- Flipchart paper
- One larger sheet of paper taped to wall in landscape orientation, with or without prepared titles. (For an example with prepared headings, see the matrix below.) The Sensitivity axis is optional in the original exercise, but critical for this one. It can be added after the initial round of brainstorming however to streamline the flow.

Relative Sensitivity	Computer	USB / External Drive	Cloud Storage	Phones, Print, etc.
High				
Moderate				
Low				

Explain to participants that we're going to conduct an information mapping activity to get a sense of where our important information actually is.

Start by listing the different places where our information is stored, according to participants. If no suggestions are forthcoming, we can prompt participants with the obvious stuff:

- Computer hard drives
- USB flash drives
- External hard drives
- Cellphones
- CDs & DVDs (and BDs)
- Our email inbox
- The Cloud: Dropbox, Google Drive, SkyDrive, etc
- Physical copies (or “hard copies”) in the office
- Multimedia: Video tapes, audio recordings, photographs, etc.

Use large stickies to place these as column headers on a wall. More will come up later in the course of the exercise.

Elicit from participants what type of information or data they have in each of these places. For example:

- Email
- Contact details, such as a member database
- Reports/research
- Funder information / contracts
- Accounts/spreadsheets
- Videos
- Images
- Private messages on Facebook, etc.

To encourage participant interaction, write one example on a sticky and place it in the appropriate box in the matrix. Then, ask whether there is another copy of this data somewhere. If there is, you can use another sticky and put it wherever they keep the duplicate.

TIP: Place Computers, Phones, and Email next to each other, so you won't have to create duplicates for everything "stored" in email (and therefore on laptops and phones)

Introduce a new vertical axis representing sensitivity. The higher on the chart, the more sensitive the data. Ask the participants to rank data.

For a large group, divide the group into smaller teams for the next steps (it helps if there are relatively clear thematic distinctions within the group, such as nationality, type of work, area of interest, etc.)

Provide stickies to the group(s). Have the group(s) brainstorm about all of the data they work with, focusing on the most important data first.

Participants should write ONE type per sticky, and create duplicates if the data is stored in multiple locations.

For a small group, this can be done as a "live" brainstorm. For larger groups that have been subdivided, have each group finish listing out their most important data and then have each group place the stickies on the matrix. Invite discussions around the sensitivity of the data.

An example may look something like this:

Level Up Backup Matrix Example

Explain that this gives us an idea of where our data is. Elicit whether or not this is all the data we generate? Of course it isn't: It's only a small percentage.

The LevelUp lesson uses this primarily to discuss the importance of backups, and this is a valuable point to make.

Call out the information that they are keeping on their computer's hard drive (which will usually be the fullest one). Elicit some of the things that can cause a computer to stop working. Maybe take a show of hands: Who has had this happen to them?

- Virus or malware attack destroyed a computer or some data
- Stolen computer, confiscated computer
- Infrastructural problems, like a power failure broke a computer
- Inexplicably bricked computer, etc.

For SAFETAG, we focus on the "Sensitive data in the wrong hands" section. Based on the clustering of sensitive data along the vertical access, choose a column that has an unsual amount of sensitive data (email or computers, usually).

Remove the stickies from the column but keep them in your hand and read them. Now I have this information. What can I do with it? And what are you left with? Is anyone at risk - yourselves? partners? If this were published on the Internet, what would happen?

Recommendation

RISKS OF DATA LOST AND FOUND

Summary

Have staff rank the impact if different data within the organization was lost, and the impact if various adversaries gained access to that data.

Overview

Materials Needed

Considerations

Walkthrough

See the Sensitive Data activity for an interactive way to gather the types of data in the organization for this ranking exercise.

Recommendation

PRIVATE DATA

Summary

Guide staff through an activity to have them list private data within the organization (e.g. Using the "personal information to keep private" handout. [14])

Overview

Materials Needed

Considerations

Walkthrough

Personal Information To Keep Private

Information that can be used to identify individuals, organizations, and even communities of practice should be treated with the utmost care. Some data, like names, phone numbers, and addresses are obvious, while others, like computer names, the MAC addresses of wifi cards, or pseudonymous social media accounts may be less obvious. Also, combinations of information - location, data, and type of activity, or even an issue area of interest and a city name may specify a very small number of activists or organizations.

This spreadsheet, part of the Responsible Data Forum documentation sprint provides a useful baseline of types of data and ways to manage or obfsucate it usefully: Data Anonymization Checklist

Recommendation

For the internal audit report back to the organization, much of the information will require specific identification of user devices (and by extension, their users), as well as very sensitive organizational data. None of this data, by intention, accident, or adversarial action, should be shared with third parties.

Please refer to the Analysis and Reporting section for the limited data set that is required for project reporting, and to the Operational Security section for guidance on data security.

ORGANIZATIONAL DEVICE USAGE

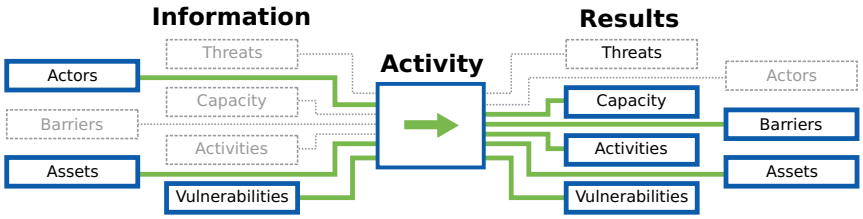
SUMMARY

During this component an auditor flags potential risks related to physical access, storage, backups, and security of the individual devices and suggests new policies and practices. It should be noted that SAFETAG is focused primarily on the digital impacts of physical assests. This guide does not provide a full physical security assessment.

PURPOSE

Because the SAFETAG framework is focused on the security of data, it's also cricial that the physicality of devices on which this data residences including the hard-wired networks through which its exchanged be not overlooked. Compromised devices have the ability to undermine nearly any other organizational attempt at securing information. Knowing if devices receive basic software and security updates/upgrades and what core protections exist against unauthorized access is vital to designing a strategy to make the host more secure.

THE FLOW OF INFORMATION



User Device Assessment Information Flow

GUIDING QUESTIONS

- Who has physical access to what? Who has remote access to what?
- When are devices not monitored by trusted staff?
- What work and personal devices do staff use to accomplish their work, store work related files, or engage in work communications?
- What organizational and external/personal services do staff use to accomplish their work, store work related files, or engage in work communications?
- How do staff communicate internal and external? What tools do they use?
- What are the existing in/formal security practices that the participants use to address risks.
- How could adversaries gain access? (forced entry, theft, social engineering, seizure)
- Are there mitigation procedures if devices are lost or taken by adversaries?

APPROACHES

- **Physical Access to Devices:** Tour the office and look for logged in devices without users, servers, network jacks, written down passwords and document how difficult it would be for a visitor or after-hours break-in to access sensitive systems. Have staff take a physical security security
- **Conduct a Hands on Device Interview/Audit:** Inspect and record information on user devices (work & personal) for security concerns (existance of passwords, patch levels, user privileges, drive encryption, ports/services running, anti-virus capabilities)
- **Password User Survey:** Have staff take the password use survey for ALL devices used for work. [15,16]

OUTPUTS

- List of all assets in the organization and whom they belong to.
- Notes on un/documented access controls measures for the office
- List of software running on staff devices and date of last update
- List of known vulnerabilities, and identifiable malware, that the office is vulnerable to.
- List of malware found by running updated anti-virus on office computers (if anti-virus installed during device inspection.)
- List of specific unsecured servers, workstations, external hard drives and any other digital resources
- Notes on existing security measures for all digital systems
- Written-down passwords

OPERATIONAL SECURITY

- Treat the information learned/collected with the utmost sensitivity and security. Physical notes should be destroyed immediately after use and digital notes should be kept in line with overall SAFETAG standards.

PREPARATION

Baseline Skills

- Basic systems administration experience for common operating systems

ACTIVITIES

GUIDED TOUR

Summary

The physical assessment methodology is focused on how to mitigate against threats that occur because of the arrangement of digital assets in the physical world.

The assessment uses a walkthrough and interview methodology to answer the following questions:

- How are daily devices used and stored?
- Where are they when employees go home?
- Are there active network jacks that are unused, are they in public spaces, are they in places where people would not notice if there was somthing plugged into them?
- How are backups managed? Where are they stored?
- Where are the servers and network components that host and manage the organizations assets?

- Who has independent access to the office space?

Overview

- Have your point of contact walk you around the office (often as part of introductions on the first day) - mentally note physical security concerns.
- Discuss access policies

Materials Needed

- A notepad may be useful

Considerations

Walkthrough

Step 1 : Guided Tour

As part of your first day, have your point of contact walk you around the office - this is primarily a chance to understand the office layout and meet the rest of the staff, but take mental note of the devices in use and laying out on desks as you walk around the office. Note as well the location and access to components such as servers and networking components.

- Device usage and storage,
- Sensitive information or external storage drives lying on desks,
- Accounts/passwords written on post-its, white-boards, etc.,
- Unattended, logged in computers,
- Unlocked cabinets, computer rooms, or wiring closets.

Taking actual notes may make the staff feel that you are judging them, so refrain from this if possible, especially if this is your first interaction.

Step 2 : Access Policies

Working with your POC and other relevant staff (administrative/operational staff, IT staff), enumerate list of everyone who has independent access to the office space, and routine after-hours access (i.e. who is able to unlock the space). This may include cleaning or other service personnel. Shared office spaces present unique challenges, and access policies and procedures for the building housing the office may also become relevant.

Materials that may be useful

PHYSICAL SECURITY SURVEY

Do you have policies and procedures for authorizing and limiting unauthorized physical access to digital systems and the facilities in which they are housed?

- [ ] No
- [ ] Yes

Do your policies and procedures specify the methods used to control physical access to your secure areas, such as door locks, access control systems, security officers, or video monitoring?

- [ ] No
- [ ] Yes

If yes, what are there?

Is access to your computing area controlled (e.g. reception or security desk, sign-in/sign-out log, temporary/visitor badges etc)?

- [ ] No
- [ ] Yes

Are visitors escorted into and out of controlled areas?

- [ ] No
- [ ] Yes

If yes, who is responsible for it?

Are your workstations inaccessible to unauthorized users (e.g. located away from public areas)?

- [ ] No
- [ ] Yes

Is your computing area and equipment physically secured? - [ ] No - [ ] Yes

If yes, how is it secured?

Are there procedures in place to prevent computers from being left in a logged on state, however briefly?

- [ ] No
- [ ] Yes

If yes, what are the procedures?

Do you have procedures for protecting data during equipment repairs?

- [ ] No
- [ ] Yes

If yes, what are the procedures?

Do you have policies covering laptop security (e.g. cable lock or secure storage)?

- [ ] No
- [ ] Yes

Do you have a business continuity plan in case of serious incidents or disaster to your digital resources and is it current?

- [ ] No
- [ ] Yes

If yes, please highlight the steps taken.

Does your plan identify areas and facilities that need to be sealed off immediately in case of an emergency?

- [ ] No
- [ ] Yes

Are key personnel aware of the plan and how to respond to the emergency?

- [ ] No
- [ ] Yes

Recommendation

Office Equipment is unsecured against burglary

Unsecured physical network components and devices such as computers, servers, and external drives present a risk of sensitive data loss through theft, seizure, and malicious interference. Access to network compontents and servers should be limited and devices should be secured when not in use.

In the event of a burglary or office raid, an attacker could easily obtain sensitive information from devices without encryption, external hard drives, and other easily accessible items. An advanced attacker could compromise the network for later surveillance.

Secure Devices

Lock in desks or via security cables all easily portable items

Any device which connects to the organization's digital assets (and therefore has passwords or cached data) or stores organizational data (including backup drives, laptops, desktops, cameras, other storage media), should be secured (ideally out of sight, such as in a locked cabinet or desk drawer) when not in use to prevent theft and discourage seizure.

Follow the Device Assessment guidelines on drive encryption.

Encrypted drives offer the best protection against data loss from stolen or seized devices. Follow the recommendations of the Device Assessment section, paying specific attention to the need for strong passwords, automatic locking of logged-in accounts, and the importance of turning a machine off to fully benefit from drive encryption.

Place core network components and servers in a locked space.

Direct access to servers and network components such as routers, cablemodems, patch panels and switches provides an adversary multiple ways to extract sensitive information and cause extensive, yet hard to detect, damage. Ensuring that not only are these physically protected, but that there are organizational policies around which staff have access to them is critical - a locked cabinet that always has the key in the lock does not provide security. If a particular component needs, for example, regular rebooting, creative solutions should be found to balance security and staff needs.

De-activate unused network ports

Hard-wired network ports tend to connect directly into the most trusted parts of a network. De-activating any that are in public areas of the office (front desk, conference rooms, break rooms), as well as any that are not needed is recommended.

DEVICE AND BEHAVIOUR ASSESSMENT

Summary

The auditor checks staff devices for updated systems and software, anti-virus and other security capabilities, and identifies software running on computers and its current version. The auditor checks for known vulnerabilities to any out of date software.

This is used to develop a report component exposing how un-updated software can lead to large vulnerabilities.

Overview

- Identify what privilege level services are running under -- Are users using accounts with admin privelges, or are they using another user and have to type in a password to get admin rights? [17]
- Check for existence and status of anti-virus (and anti-malware tools) on the device. [18]
- Record the version and patch levels of software on the device. [19]
- Identify what level of encryption is being used and is available for data storage on the device. [20]
- Using the list of software versions and patches identify attacks and, if possible, identified malware that devices in the office are vulnerable to.

Materials Needed

- A notepad may be useful

Considerations

- Communicate with the staff members the level of confidentiality you are treating discussions around their device and technology usage with - i.e. explain what incident response triggers you have agreed upon with the organization, and that anything not triggering that is to be only reported in aggregate.

Walkthrough

The auditor inspects a subset of key and/or representative user devices (work & personal). The auditor should focus on the work devices to limit scope creep, but if the office has many personal devices accessing organizational accounts/data, the auditor should share what "red flags" they are looking for and work in tandem with device owners and/or IT staff. For a small office, it may be possible to check every machine. For larger offices, the auditor should use a subset to get a feel for the overall security stance of user devices.

As you work with staff members, also interview them about the other devices they use such as phones and tablets, and how they connect to work services - email/webmail, chat Apps, intra/extranet tools, Constituent Relationship Management (CRM) tools like CiviCRM or Salesforce, financial tracking tools, and website management tools.

Recommendation

If Unsupported Operating System - Upgrade to Recent Version

Popular operating systems like Windows XP are, sadly, no longer receiving security updates. Upgrade to the latest version keeping in mind the system requirements of the version selected

If Pirated Software - Move to Licensed Software Systems

While "pirated" operating systems and software are extremely common (especially for Windows) they often leave much to be desired in terms of security. If the OS or Software is not receiving regular updates from the software creator, it is extremely vulnerable to thousands of potential attacks. Switch to licensed software or recommended Free Open Source Software

If Outdated - Update Operating Systems and Other Software

Operating Systems and Softwares of all varieties - Windows, Mac, Linux, and others, are constantly being updated. These updates often fix bugs, but they also protect the system from newly discovered vulnerabilities. It can seem difficult to keep updating constantly, but this is very important to protect even non-sensitive systems.

If Vulnerable Software - Update Vulnerable Software

Many critical software components, such as Java or Adobe Flash, have many vulnerabilities and need to be aggressively updated. If there are not needed for work by the users, uninstall them

If No Anti-Virus and Anti-Malware Scanner - Install Anti-Virus and Anti-Maware Scanner

An Anti-virus and Anti-malware offer some minimal protection to the system and therefore is important to have them installed.

If Outdated Anti-Virus - Update Anti-Virus

Most AV tools automatically update, but this can sometimes get out of sync, or if the AV was a pre-installed trial system, it will stop updating after its trial period. An out of date anti-virus is worthless. Therefore ensure that continuous udpdating of AV is done.

If Unencrypted Drive - Encrypt Hard Drives

If Inactive firewall - Activate both personal and server firewall (If present)

PASSWORD SECURITY SURVEY

Summary

WEAK PASSWORDS

Weak and "shared" passwords are prevalent - even after hundreds of well-publicized global password breaches, "password" and "12345" remain the most popular passwords. Weak wifi passwords are specifically a challenge, as wifi signals often are accessible outside of an office's physical limits, but provide full access to the private network.

Overview

- Using the password survey, determine the organization's baseline for password security
- If relevant, test the wireless network's password strength

Materials Needed

- For the (most common) WPA password-based attacks, an already-prepared dictionary of words to use to attack the password will be required. See the Appendix on Audit Preparation for guidance on dictionary preparation.
- A Password Survey (see Appendix) for an alternate way to gather password practices
- The Level Up Activity, Password Reverse Race provides a staff activity.

Considerations

Materials that may be useful

PASSWORD SURVEY

How many passwords do you have to remember for accounts and devices used to do your work?

- [ ] No
- [ ] Yes

If you tried to login to your computer account right now, how many attempts do you think it would take?

- [ ] No
- [ ] Yes

To how many people have you given your current password?

- [ ] No
- [ ] Yes

Have you ever forgotten your current password?

- [ ] No
- [ ] Yes

If yes, how did you recover it?

Have you ever forgotten old work passwords?

- [ ] No
- [ ] Yes

If yes, how did you recover it?

When you created your current password, which of the following did you do?

- [ ] I reused an old password
- [ ] I modified an old password
- [ ] I reused a password I was already using for a different account
- [ ] I created an entirely new password
- [ ] Other:

Did you use any of the following strategies to create your current password (choose all that apply) ?

- [ ] Password based on the first letter of each word in a phrase
- [ ] Based on the name of someone or something
- [ ] Based on a word or name with numbers / symbols added to beginning or end
- [ ] Based on a word or name with numbers and symbols substituting for some of the letters (e.g. '@' instead of 'a')
- [ ] Based on a word or name with letters missing
- [ ] Based on a word in a language other than English
- [ ] Based on a phone number
- [ ] Based on an address
- [ ] Based on a birthday

How long is your current password (total number of characters)?

- [ ] I prefer not to answer.

What symbols (characters other than letters and numbers) are in your password?

- [ ] I prefer not to answer.

How many lower-case letters are in your current password?

- [ ] I prefer not to answer.

How many upper-case letters are in your current password?

- [ ] I prefer not to answer.

In which positions in your password are the numbers?

- [ ] I prefer not to answer.
- [ ] First
- [ ] Second
- [ ] Second from last
- [ ] Last
- [ ] No Numbers
- [ ] I prefer not to answer.

In which positions in your password are the symbols?

- [ ] I prefer not to answer.
- [ ] First
- [ ] Second
- [ ] Second from last
- [ ] Last
- [ ] No Numbers
- [ ] I prefer not to answer.

Have you written down your current password?

- [ ] No
- [ ] Yes, on paper
- [ ] Yes, electronically (stored in computer, phone, etc.)
- [ ] Other

If you wrote down your current password how is it protected (choose all that apply) ?

- [ ] I do not protect it
- [ ] I stored it in an encrypted file
- [ ] I hid it
- [ ] I stored it on a computer or device protected with another password
- [ ] I locked up the paper
- [ ] I always keep the password with me
- [ ] I wrote down a reminder instead of the actual password
- [ ] Other

Do you have a set of passwords you reuse in different places?

- [ ] No
- [ ] Yes

Do you have a password that you use for different accounts with a slight modification for each account?

- [ ] No
- [ ] Yes

Recommendation

RECOMMENDATION: ADOPT STRONGER PASSWORDS

Any important password should be long enough and complex enough to prevent both standard dictionary attacks and “brute-force attacks” in which clusters of powerful computers work in parallel to test every possible character combination. (We recommend 12 or more completely random characters or a passphrase that contains five or more relatively uncommon words.) The key should not contain common “phrases,” expecially from well known literature like Shakespeare or religious texts, but also should not include number sequences or phrases, especially if they are related to the organization, its employees or its work.

Specifically for wireless passwords, choosing a strong WPA key is one of the most important steps toward defending an organization’s network perimeter from an adversary with the ability to spend some time in the vicinity of the offices. By extension, mitigating this vulnerability is critical to the protection of employees and partners (and confidential data) from the sort of persistent exposure that eventually brings down even the most well-secured information systems.

Because shared keys inevitably end up being written on whiteboards, given to office visitors and emailed to partners, the WPA key should also be changed periodically. This does not have to happen frequently, but anything less than three or four times per year may be unsafe.

RESOURCES

- *Guidelines:* "Guidelines on Firewalls and Firewall Policy" (NIST 800-41)
- *Benchmarks:* "Security Configuration Benchmarks" (CIS Security Benchmarks)
- *Repository:* "National Checklist Program Repository - Prose security checklists" (National Vulnerability Database)
- *Security Guidance:* "Operating Systems Security Guidance" (NSA)

Password Security

- *Guide:* "How to Teach Humans to Remember Really Complex Passwords" (Wired)
- *Guide:* "Security on Passwords and User Awareness" (HashTag Security)
- *Video:* "What’s wrong with your pa$$w0rd?" (TED)
- *Article:* "Password Security: Why the horse battery staple is not correct" (Diogo Mónica)
- *Organization:* "Passwords Research" (The CyLab Usable Privacy and Security Laboratory (CUPS))

Privilege Separation Across OS

- identify what privileges services are running as
- identify is the admin user is called admin or root
- Identify if users are logging in and installing software as admin.

Examining Firewalls Across OS

- *Checklist:* "Firewall Configuration Checklist." (NetSPI)

Identifying Software Versions

Device Encryption By OS

- Identifying if a device is using encryption by OS
- Encryption availablility by OS
- Encryption Guides

Anti-Virus Updates

Identifying Odd/One-Off Services

- *Guide:* "Physical Penetration Test" (About The Penetration Testing Execution Standard)
- *Checklist:* "Check list: Office Security" (Frontline Defenders)
- *Manual:* Planning, improving and checking security in offices and homes
- *Guide:* "Physical Security Assessment - pg. 122" (OSTTM)

Follow up and Reporting

DEBRIEF

SUMMARY

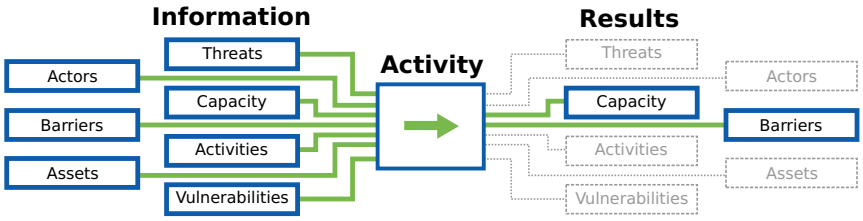
This component consists of an out-brief to key points of contact, providing basic pressure relief through group and individual interactions, and planning future follow-up with the host and key individuals.

PURPOSE

SAFETAG is an auditing framework designed to connect small civil society organizations and independent media outlets to the digital security services they need. But, more than that it is designed to provide audits that increase an organization's agency to seek out and address security challenges independently. This can be an auditor's last in-person chance to engage with the staff to shape their perspective of the audit.

The debrief allows the auditor to ensure that they leave the host and its staff ready to start addressing their digital security. By providing some immediate outcomes to the host and its staff, and in combination with training or security consultation in the Responsive Support section, the auditor can ensure that the host sees the audit as a guide instead of a condemnation.

THE FLOW OF INFORMATION



Debrief Information Flow

GUIDING QUESTIONS

- Is the organization empowered to make changes?
- Do key personnel have a general understanding of the initial findings?
- Does the organization understand the next steps of the audit process?

APPROACHES

- Discuss next steps and points of contact going forward for the host.
- Provide psycho-social care and re-framing as needed.
- Initiate follow-up with host (organizational and individual).

OUTPUTS

- A date scheduled for sending in the report.
- Additional points of contact (with identified secure communications channels) if needed.

OPERATIONAL SECURITY

PREPARATION

RESOURCES

- *Resource:* The Psychological Underpinnings of Security Training (Craig Higson-Smith)
- *Article:* "No money, no problem: Building a security awareness program on a shoestring budget"

Facilitation Preparation

- *Tip Sheet:* Facilitator Preparation Tips (Integrated Security)
- *Guidelines:* "Facilitator Guidelines" (Aspiration Tech)
- *Guide:* "Session_Design" (Aspiration Tech)
- *Kit:* "Resource Kit" (eQualit.ie)
- *Questions:* "Pre-Event_Questions" (Aspiration Tech)
- *Guide:* "Break Outs" (Aspiration Tech)
- *Resources:* "Be a Better Trainer" (Level-up)

ACTIVITIES

FOLLOW UP

SUMMARY

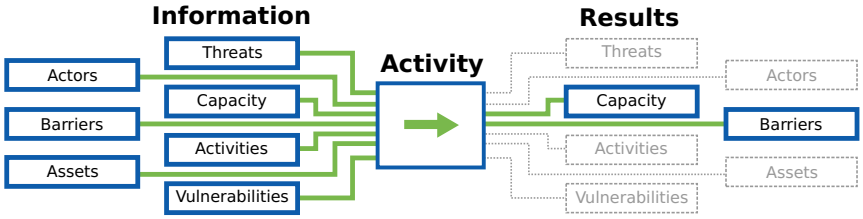
This component allows an auditor to explain and get feedback on their report as well as evaluate the success of the process over time through a continued relationship with the host.

This component consists of the final meeting with the host and following up with them after a period of a few months to see if they need further assistance, are willing to share their experience working with any of the recommended resources, or as new resources are identified.

PURPOSE

Follow up can be a valuable tool for encouraging an organization to continue their digital security process. But, follow up needs to be desired by an organization and achievable for the auditor. As such, follow up must be minimally intrusive on both the auditor and the host's time.

THE FLOW OF INFORMATION



Information Flow

GUIDING QUESTIONS

- What are the barriers the organization faced in implementing the recommended risk mitigation plan?
- Are there new resources that the auditor can provide to supplement the original audit?
- What can you do to make your follow up perceived as additional support instead of as an evaluation of their success?

APPROACHES

- **Staff Feedback Survey:** Receive feedback from the staff on the execution of the audit.
- **Report Follow Up Meeting:** Have a follow-up call to discuss report.
- **Making Introductions:** Introduce organization to known resources as needed.
- **Long-Term Follow Up:** Contact host after a few months to check on progress, get long-term feedback and connect with any new resources.

RECOMMENDATION DEVELOPMENT

SUMMARY

In this component the auditor identifies the organization's strengths and weakness (expertise, finance, willingness to learn, staff time, etc.) to adopting new digital and physical security practices and documents the possible actions the organization could take on to address the vulnerabilities found during the audit, the difficulty of taking on those actions, and the resources that the host may be able to leverage to address them. Resources can include, but are not limited to, local technical support and incident response groups/trade organizations, places to obtain discount software, trainers, and guides/resrouces they can use to support their up-skilling.

PURPOSE

The host needs to be able to take action after an audit. The recommendations that an auditor provides to address vulnerabilities must cover a range that allows an organization to address them in both the short-term and more comprehensively in the long-term. Knowing an organization's strengths and weaknesses will allow the auditor to provide more tailored recommendations that an organization will be more likely to attempt and achieve. In doing this the SAFETAG auditor has an opportunity to act as a trusted conduit between civil society organizations in need and organizations providing digital security training, technological support, legal assistance, and incident response.

GUIDING QUESTIONS

- What are the organizational areas of strength (expertise, finance, willingness to learn, staff time, etc.) that the organization can leverage when engaging in technological adoption/change?
- What are the organizational areas of weakness (expertise, finance, willingness to learn, staff time, etc.) that need to be taken into consideration when engaging in technological adoption/change?
- What are the organizational barriers to adoption?
- Are the recommendations you are providing directly related to the security audit? If not, do they support the organization in accomplishing their security tasks, or distract from them?

APPROACHES

- **Identify and Explain Un-Addressed Concerns :** Write explanations for why any adversaries or threats that the auditor identifies as "un-addressable" with the organizations current capacity.
- **Identify Recommendations:** Identify possible actions to address each vulnerability.
- **Identify Useful Resources:** Identify resources that the organization can leverage to accomplish the identified recommendations.

ROADMAP DEVELOPMENT

SUMMARY

This component consists of an auditor sorting their recommendations in relation to the organizations threats and capacity. The auditor prioritizes vulnerabilities, weighs the implementation costs of recommendations and then creates an actionable roadmap for the organization to make their own informed choices about possible next steps as they move forward.

PURPOSE

As part of SAFETAG's dedication to building agency and supporting organizational adoption of safer practices, a careful prioritization of vulnerabilities is invaluable in keeping audit results from appearing overwhelming. An organization needs to be able to weigh their possible paths forward against the time lost from program activities, the cost to implement the threat, and the other threats that they are not addressing. Roadmapping is used to give the host the tools to make these decisions and provide them with a recommended path forward that will allow them to make immediate gains towards protecting themselves. The existing in/formal security practices captured during this process will be used to remove organizational and psyco-social barriers to starting new practices.

GUIDING QUESTIONS

- Compare the resources required against the capabilities identified in the risk modeling activities and the contextual research you completed.
- Based upon the organizational capacity assessment, build a menu that builds upon the organizational strengths to create a path forward that provides achievable outcomes, maintains agency, and steps towards long-term difficult outcomes with high reward for the host.

APPROACHES

- **Risk Matrix Development:** Create a risk matrix that maps each vulnerability found to its likelihood and impact.
- **Implementation Matrix Development:** Create an "implementation matrix." with the urgency of the threat addressed balanced by the difficulty of implementation given available organizational capacity for the recommendations.
- **Roadmap Development:** Identify critical vulnerabilities, with achievable recommendations that fit into threat narratives that you heard from staff during the audit to create a remediation roadmap for addressing the threats faced by the organization.
- **Documenting Existing Success':** Place the recommendations on a time-line that includes the existing practices of the organization to show that the remediation process is a continuation of the hosts existing in/formal security practices. [21]

REPORT CREATION

"*A good analysis might turn the threats into stories so they stay close to mind as software is being written or reviewed. A good story contains conflict, and conflict has sides. In this case, you are on one side, and an attacker is the other side.*" - *Threat Modeling: Designing for Security* [22]

SUMMARY

This component consists of an auditor compiling their audit notes and recommendations into a comprehensive set of documents the shows the current state of security, the process by which the auditor came to that assessment, and recommendations that will guide the hosts progression to meet their security goals.

PURPOSE

Once an auditor has left, the report is the auditor's chance to continue a conversation (albeit a static one) -- even if the organization never talks to the auditor again. If written with care it can be a tool to encourage agency and guide adoption. The report has many audiences who will need to use it in different ways. For the auditor and the organization, it acts as documentation of what an auditor accomplished. For the organization, it will be guide for connecting vulnerabilities to actual risks, a rallying cry for change, and proof of need for funders. For those the organization brings in to support their digital security, it provides a roadmap towards that implementation and a task-list for future technologists and trainers paid to get the host there - as well as a checklist for validating that threats have been addressed.

BASELINE SKILLS

PREPARATION

MATERIALS NEEDED

APPROACH

- Create charts and visuals for roadmap, risk-matrix, implementation matrix, and critical processes.
- Compile approaches, impact, risk, recommendations and resources for each vulnerability.
- Prepare narrative components.
- Collect agreements & scope.
- Document tools used for testing where needed.
- Update glossary where needed.
- Compile full report contents.
- Send the report to client. [23]

OUTPUTS

- A completed report delivered securely to the organizational point of contact.
- Documented process examples to submit back to SAFETAG.

OPERATIONAL SECURITY

- Treat the report with the utmost security. It should only be shared as a complete work between the auditor(s) and the identified leadership and points of contact of the organization.

RESOURCES

- *Guide:* "Reporting" (The Penetration Testing Execution Standard)
- *Guide:* "The Art of Writing Penetration Test Reports" (INFOSEC Institute)
- *Guide:* "Writing a Penetration Testing Report" (SANS)
- *Guide:* "Wow your client with a winning penetration testing report" (Tech Target)

ACTIVITIES

Footnotes

1. " Some activities common in penetration tests may violate local laws. For this reason, it is advised to check the legality of common pentest tasks in the location where the work is to be performed."↩
2. " Some activities common in penetration tests may violate local laws. For this reason, it is advised to check the legality of common pentest tasks in the location where the work is to be performed."↩
3. "In addition, some service providers require advance notice and/or separate permission prior to testing their systems. For example, Amazon has an online request form that must be completed, and the request must be approved before scanning any hosts on their cloud. If this is required, it should be part of the document."↩
4. NIST SP 800-115, Technical Guide to Information Security Testing and Assessment. Section 7.1 Coordination↩
5. "Obviously, being able to get in touch with the customer or target organization in an emergency is vital."↩
6. See the auditor trainee resource list↩
7. The auditor travel kit checklist can be found in the SAFETAG "full guide."↩
8. ^NIST_SP_800-115-travel_prep↩
9. Event Planning Inputs - Level-Up↩
10. "CSOs should gradually build a culture in which all staff, regardless of technical background, feel some responsibility for their own digital hygiene. While staff need not become technical experts, CSOs should attempt to raise the awareness of every staff member, from executive directors to interns - groups are only as strong as their weakest link—so that they can spot issues, reduce vulnerabilities, know where to go for further help, and educate others."↩
11. "Impacts: Chapter 2.7 p. 46 - Operational Security Management in Violent Environments"↩
12. "Likelihood: Chapter 2.7 p. 47 - Operational Security Management in Violent Environments"↩
13. The "personal information to keep private" handout can be found in the SAFETAG "full guide."↩
14. The "personal information to keep private" handout can be found in the SAFETAG "full guide."↩
15. The password Survey can be found in the SAFETAG "full guide."↩
16. The "password security: guides and manuals" resources list can be found in the SAFETAG "full guide."↩
17. Privilege Separation Across OS↩
18. Anti-Virus Updates↩
19. Identifying Software Versions↩
20. Device Encryption By OS Type↩
21. See: "Threat Modeling: Designing for Security" by Adam Shostack, p. 298.↩
22. See: "Threat Modeling: Designing for Security" by Adam Shostack, p. 401.↩
23. "When a pilot lands an airliner, their job isn’t over. They still have to navigate the myriad of taxiways and park at the gate safely. The same is true of you and your pen test reports, just because its finished doesn't mean you can switch off entirely. You still have to get the report out to the client, and you have to do so securely. Electronic distribution using public key cryptography is probably the best option, but not always possible. If symmetric encryption is to be used, a strong key should be used and must be transmitted out of band. Under no circumstances should a report be transmitted unencrypted. It all sounds like common sense, but all too often people fall down at the final hurdle." - The Art of Writing Penetration Test Reports↩