****

Learner and environmental analysis (LEA), Task Analysis (TA), and Learning requirements analysis (LRA) prepared for:

POPP3R Cybersecurity

by:

Dan Lara, Mariola Diawara, Midori Connolly

OPWL 537 Instructional Design

Boise State University

Fall 2023

****

[**Project assumptions 1**](#_heading=)

[**Project focus 1**](#_heading=)

[Organizational description and mission 1](#_heading=h.ktonuwuq3o1q)

[Socio-physical Context 1](#_heading=h.203juxc94tdm)

[Overview of Problem to be Addressed 1](#_heading=h.nu9wuaakexfu)

[Outcome-level Performance and Causes 2](#_heading=h.tqw6ur8a4g1n)

[Desired Outcomes 3](#_heading=h.8dwek8wv35ac)

[**Learner and Environmental Analysis (LEA) 4**](#_heading=)

[Data Collection 4](#_heading=h.lflpsdbmqmqp)

[Cognitive Characteristics of Learners 4](#_heading=h.g6bfx7y14ald)

[Learner Demographics 4](#_heading=h.o6nuy27xy2pm)

[Physical Characteristics 5](#_heading=h.er4t6dlh8wj)

[Affective Characteristics 5](#_heading=h.2q7mbvcwkiqs)

[Socio-cultural Characteristics 5](#_heading=h.aj3i25ir2vt5)

[Prior Knowledge 6](#_heading=h.jc4p89pdvcos)

[Potential for Learner Motivation 6](#_heading=h.5lfku08m1b13)

[Potential Limitations to Instruction/Training 6](#_heading=h.o9i947uppotf)

[**Task Analysis (TA) 7**](#_heading=)

[Data Sources 7](#_heading=h.3dy6vkm)

[Difficulty, Complexity, and Criticality of the Tasks 7](#_heading=h.ca3hckopmyil)

[Task Initiation, Duration, Method, Frequency 7](#_heading=h.wy9k0ieaxaaf)

[Task Breakdown 8](#_heading=h.zcqaiu7ysbp7)

[**Learning Requirements Analysis (LRA) 12**](#_heading=)

[Training Configuration 13](#_heading=h.rhpdazuz2ejc)

[Planned Configuration 13](#_heading=h.2s8eyo1)

[**References 14**](#_heading=h.2vmj6vhob0pj)

# Project assumptions

* A needs assessment has revealed that performance-based learning and development intervention is needed because the root cause of a worthy performance gap is a lack of knowledge, skills, and attitude
* Adequate sponsorship exists for the project.

# Project focus

## Organizational description and mission

Popp3r Cybersecurity is a small business cyber consultancy based in Winnipeg, Canada. Their vision is to provide their clients with world-class, unparalleled protection against cybercrime by leveraging Innovation, Integrity, and Ingenuity.

Where large companies and enterprises are using different tools and techniques to train their staff against threats, Popp3r Cybersecurity wants to provide the same kind of services to smaller companies, non-profits, and small municipalities, given that 60 Percent of small businesses will fall after a breach.

Popp3r’s purpose is to cybersecure every client, by providing expert advice and outstanding service.

## Socio-physical Context

Popp3r Cybersecurity is a consulting boutique practice, based in Winnipeg, Manitoba. They strategically partner with several of the most respected security technology firms in Canada and abroad, offering their clients access to a broad portfolio of industry-leading cyber solutions best suited to protect their reputation, assets, and people.

Apart from awareness training, Popp3r Cybersecurity provides virtual CISO services for small companies unable to afford a CISO internally, including non-profits. They are certified by the government of Canada to provide cybersecurity services to small businesses paid for by the government.

The number of staff is currently four, which includes internships. The founder, Hernan Popper, desires to build a cyber awareness lesson that he can provide to nonprofits and small organizations free of charge.

All organizations encounter operational dangers, including system interruptions or malfunctions, breaches in security or data privacy, cyberattacks, human mistakes, and failure to protect personal data. Additionally, modifications in operational procedures or insufficient controls, even involving third parties they collaborate with, can disrupt their business. These risks can tarnish the organization's reputation, negatively influencing its operational outcomes, financial status, and cash flow.

Each year companies face an influx of new staff who need to identify these risks and vulnerabilities, learn how to effectively manage and act on the above-mentioned risks and vulnerabilities, and know where to turn for help when needed during their daily work activities.

## Overview of Problem to be Addressed

Small to medium-sized businesses (SMBs) and non-profits manage sensitive data, often including personal and financial details of employees, volunteers, clients, donors, and partners. Because this data is enticing to malicious actors, it's crucial for these smaller and non-profit entities to fortify their cybersecurity defenses.

**1. Protect Sensitive Data:** SMBs and non-profits deal with financial data such as transactions, credit information, and personal identifiers. This data, if accessed unlawfully, can result in significant financial loss, identity theft, and various forms of fraud.

* **Typical Performance:** Many organizations, regardless of size, have implemented basic security measures to protect sensitive data. However, the degree of protection varies, and smaller entities may lack advanced security due to limited resources.

**2. Regulatory Compliance:** Like larger counterparts, SMBs and non-profits are bound by local, national, and sometimes international regulations requiring the protection of consumer data. Failure to comply can result in severe penalties, sanctions, and legal consequences.

* **Typical Performance:** Compliance levels tend to be higher among organizations that are under strict regulatory environments. Nonetheless, smaller businesses and non-profits may struggle to keep up with the ever-changing landscape of regulations due to lack of expertise and resources.

**3. Maintain Trust:** Clients, employees, donors, and volunteers entrust their personal and financial information to SMBs and non-profits. A breach in security can swiftly erode the trust established with clients, leading to the loss of both customers and reputation.

* **Typical Performance:** Trust maintenance is often a priority, but the effectiveness in doing so is mixed. While larger organizations might have dedicated PR and crisis management teams, SMBs and non-profits might find it challenging to rebuild trust post-breach.

**4. Prevent Financial Loss:** Financial losses from a cyberattack are not exclusive to fraud. SMBs and non-profits can also face direct penalties, expensive legal battles, and costs associated with damage control and recovery efforts.

* **Typical Performance:** Preventing financial loss is critical for all. Larger organizations typically have more sophisticated mechanisms to mitigate financial losses, while smaller ones may lack the necessary infrastructure and might be more vulnerable.

**5. Business Continuity:** Attacks such as ransomware can stop operations in their tracks. Training staff in cybersecurity can play a pivotal role in both preventing such attacks and responding efficiently when they occur.

* **Typical Performance:** Business continuity planning is often found in larger organizations, though it's increasingly being adopted by SMBs and non-profits. However, the latter may not always have comprehensive plans or frequent training and drills.

**6. Evolving Threat Landscape:** The tactics deployed by cybercriminals are constantly changing. Keeping staff updated on the latest threats, and how to mitigate them, is essential for the security of SMBs and non-profits.

* **Typical Performance:** Awareness of the evolving threat landscape varies. Larger organizations often have dedicated cybersecurity teams staying abreast of the latest threats, whereas smaller entities may rely on external consultants or may not be fully aware of the emerging risks.

#### Outcome-level Performance and Causes

* Over 30% of workers fail phishing simulations when they do not receive training (Huisman, n.d.).
* Attachments of documents with personal data and sensitive personal data are sent via email rather than secure links.
* Access rights are cloned, and users don’t actively downgrade their access rights.
* Passwords are frequently reused and shared
* Staff send work related emails and documents to their private accounts to be able to print/work from home. Save it to their personal devices.
* Remote working and shared office spaces leave vulnerabilities in talking about confidential or sensitive information or leaving devices exposed
* Human error significantly contributes to cybersecurity breaches, being the primary culprit behind 85% of these incidents in 2022 (Tessian, 2022).

####

#### Desired Outcomes

* Pause before you click.
* Report security incidents
* Protect your own and others’ identity.
* Verify before sharing information.
* Practice awareness and vigilance in public spaces for a safe experience.
* Reserve discussions about private and sensitive work-related information for secure and private environments.
* Allow only authorized personnel entrance to office area, ensuring a secure environment for all.

Changes should occur in knowledge, skills, and attitudes.

1. Understand what a threat is so that they can identify and avoid it.
2. Know what to DO if there is an incident.
3. Become a worker who cares about improving security.

# Learner and Environmental Analysis (LEA)

#### Data Collection

* Interviews with client and SME
* Industry data and standards documentation

#### Cognitive Characteristics of Learners

Upon joining a new organization and preparing for cybersecurity onboarding training, learners typically exhibit a diverse range of cognitive characteristics and prior knowledge. Their aptitudes and academic preparation in information security can vary widely, ranging from novices with limited understanding to experienced individuals with a comprehensive grasp of the subject.

Employees may come from various job categories, each with different levels of familiarity and expertise with cybersecurity principles and practices. Their sustained attention and information processing speed during training can also differ based on their background, previous exposure to the topic, and inherent cognitive traits. Some may quickly recognize patterns and grasp new concepts due to past experience, similar processes that make the information easy to grasp or natural inclination, while others may require more time to absorb and understand the information presented. This diversity in cognitive characteristics necessitates a flexible and inclusive approach to cybersecurity training that can cater to the unique learning needs and paces of all participants.

The diversity in cognitive characteristics and potential limitations of new hires necessitates a tailored approach in designing cybersecurity onboarding tasks. Implementing adaptive learning strategies is crucial, providing foundational knowledge for beginners while offering advanced challenges for experienced individuals. Training modules should be engaging and interactive, accommodating various learning paces and styles. Incorporating a blend of theoretical and practical tasks, the program should facilitate hands-on experience, problem-solving exercises, and real-life scenarios to enhance understanding and retention. This approach ensures that each participant, regardless of their prior knowledge or cognitive traits, can grasp the essential cybersecurity concepts and skills effectively.

#### Learner Demographics

Learners in a cybersecurity onboarding program often represent a wide age range, from recent graduates in their early 20s to experienced professionals possibly in their 50s or 60s. The gender distribution reflects the broader non-profit and SMB current demographics but exact distribution is unknown at this time. The participants may come from diverse ethnic and cultural backgrounds, bringing different perspectives and approaches to problem-solving in the cybersecurity landscape. Additionally, they might possess varying levels of education and certifications, ranging from those holding diplomas and bachelor’s degrees to others with master’s degrees and specialized certificates in information technology and security.

The demographic characteristics outlined, including age, gender distribution, ethnicity, and educational background, necessitate a more inclusive and diverse approach to developing targeted cybersecurity onboarding tasks. Designing training modules that are accessible and engaging for all ages is vital, considering the wide age range; this will involve incorporating various technological tools and platforms that cater to different tech proficiency levels, and design with a mobile-first mindset.

The ethnic and cultural diversity among learners implies that training should be culturally sensitive and inclusive, avoiding jargon, examples, or references that may not be universally understood or appreciated. The varied educational backgrounds require a curriculum that is flexible enough to offer value to those with different knowledge levels, perhaps through a tiered or modular training system that allows learners to engage with content that matches their experience and expertise.

#### Physical Characteristics

Learners display diverse physical characteristics, with varied sensory and motor abilities, necessitating accessible training materials and environments to accommodate all participants effectively.

The varied physical characteristics and potential limitations among learners demand training tasks designed with accessibility and inclusivity in mind. This means incorporating adaptive technologies, providing materials in various formats (like audio, visual, and tactile), and considering ergonomic factors to ensure comfortable and effective learning for individuals with different sensory and motor abilities. Techniques might include using clear visuals, providing transcripts for audio materials, implementing hands-on practical exercises, and creating an environment where learners can engage with the content comfortably and effectively, regardless of their physical characteristics.

#### Affective Characteristics

For individuals not in the cybersecurity industry, their affective characteristics may encompass a mix of interest levels, motivations, and attitudes towards the subject matter. Many might exhibit initial anxiety or apprehension due to a lack of familiarity with cybersecurity concepts, possibly perceiving them as complex or overly technical. Their interest in cybersecurity can vary, with some showing eagerness to learn due to the relevance and importance of the topic in today’s digital age, while others might need additional motivational elements to engage.

Attitudes toward the subject matter can be influenced by previous experiences, existing beliefs about technology and security, and the perceived difficulty of the content. This could be positive and negative. The learners’ locus of control might lean external, as they may feel that cybersecurity is a specialized field controlled by experts, leading to a potential reluctance to fully engage without encouragement and support to empower them. Understanding these affective characteristics is crucial to foster a positive and conducive learning environment, easing anxieties and actively engaging and motivating all participants.

Given learners’ varied affective traits, training design should ease anxiety with straightforward language and engaging examples. Interactive modules, possibly using gamification, can spark interest and motivation. Highlighting cybersecurity's relevance through real stories can address diverse attitudes, emphasizing its importance for personal and organizational safety. For those feeling they lack control, it’s vital to showcase that everyone plays a part in cybersecurity, empowering participation and engagement from all.

#### Socio-cultural Characteristics

Learners come from varied socio-cultural backgrounds, influencing their interaction with peers and authority. Some may value cooperation and collective effort due to cultural emphasis on community, while others might lean towards individualism and competition. Attitudes towards authority figures can range, with some showing deference, while others approach with equality and openness. Cultural factors, including language, and communication styles, significantly impact their engagement and comprehension during training. Additionally, learners may have different role models and influencers shaping their aspirations and attitudes towards cybersecurity, further diversifying the group's dynamics and expectations during the onboarding process.

Socio-cultural diversity requires tailored training strategies. Different approaches to authority and peer interaction necessitate a flexible learning environment that respects hierarchical sensitivities while promoting collaboration. Training must accommodate varied communication styles, possibly through offering multilingual resources and considering cultural nuances in content delivery. Acknowledging and incorporating learners’ diverse role models and influences in cybersecurity can also help make training relatable and engaging for all participants.

#### Prior Knowledge

At this point, it can be assumed that learners will have widely varying knowledge of the subject matter. Please see *Affective Characteristics* for more information.

#### Potential for Learner Motivation

Learners potentially believe cyber security is:

* Something that is resolved by systems and technology
* An extra task on top of normal workload
* Complicated
* Won’t happen to them
* Or could find it really cool and already like to spread the cybersecurity love (lock screens of colleagues, etc)

Because cybersecurity might be intimidating or alien to many learners, creating an emotional connection to assist with their motivation to learn more and perform as desired will be critical.

#### Potential Limitations to Instruction/Training

For non-profit organizations and small-medium businesses (SMBs), the learning environment's factors affecting training include limited resources and budget constraints, which is Popp3r Cybersecurity’s main motivation to work with this group. When you remove the budget restraints, people are more open in doing more for cybersecurity. Such factors typically restrict access to cutting-edge cybersecurity tools and platforms. There’s often a diverse workforce with varied skill levels and learning needs, requiring adaptable and inclusive instructional designs. The fast-paced and dynamic work environment in SMBs demands flexible training schedules and formats, allowing employees to balance their learning with their work commitments.

Additionally, there might be a lack of dedicated personnel or departments for training, leading to dependency on external consultants or self-directed learning initiatives.

The constraints and characteristics within non-profits and SMBs necessitate cost-effective, flexible, and inclusive training strategies. Limited resources mean utilizing affordable, yet effective, training tools and perhaps leveraging free or open-source platforms. The diverse skill levels require a modular training approach, accommodating different learning needs and prior knowledge. With the dynamic work environment, training should be concise, engaging, and offered in various formats, possibly including micro-learning, webinars, and hands-on sessions, to suit different schedules and learning preferences. Dependency on external resources implies the need for easy-to-follow, self-paced learning modules that employees can navigate independently, with support available as needed.

# Task Analysis (TA)

Our Task Analysis consists of analyzing the following core competencies that combined together characterize secure behavior. By successfully completing the following tasks, the learner will secure themselves and their workplace against cyber threats.

* Creating strong passwords and using Multifactor Authentication (MFA)
* Employing safe data practices
* Protecting against computer/physical theft
* Identifying and acting on phishing
* Applying best practices to using removable media
* Identifying vishing/fraudulent calls
* Using adequate safety measures while browsing the Internet
* Taking the correct precautions when working remotely on wireless networks

#### Data Sources

We obtained data for our analysis through a combination of:

* Interviews with the customer/SMEs, Hernan Popper and Kyla Trinidad
* Reviewing existing course materials produced by the National Cybersecurity Alliance
* Personal experiences as an expert and consultant in the Cybersecurity domain

#### Difficulty, Complexity, and Criticality of the Tasks

While the tasks presented are primarily quite straightforward and will not be difficult for the majority of the audience, there will be some percentage of the audience that may lack basic digital competency or feel some intimidation when it comes to technology.

The outcome of not performing the tasks correctly could potentially result in any number of severe consequences, ranging from identity theft, business disruption and financial loss, or even a threat to personal safety.

#### Task Initiation, Duration, Method, Frequency

Anytime the learner engages with a digital device, and for as long as they are using the device, they will need to perform the prescribed tasks. Examples include:

* Checking email
* Browsing the Internet
* Answering a phone
* Working remotely
* Carrying a mobile device or laptop
* Creating a spreadsheet, uploading a file, visiting social networking sites, etc.

The only indication that a learner has completed the task correctly is the lack of a breach. They will not receive immediate feedback to know if they are meeting performance expectations.

#### Task Breakdown

1. Create a password
	1. Identify all accounts that need a password
	2. Login to each account and go to the “Change Password” feature
	3. When creating the password:
		1. Think about a phrase or sentence that is meaningful to you, such as "I love to read."
		2. Use a combination of upper and lowercase letters, numbers, and symbols to create a password from your phrase or sentence, such as "ILove2Read!".
		3. Make sure your password is at least 12 characters long.
		4. Avoid using common words, phrases, or personal information in your password.
	4. Use a password manager to store your password for your new email account.
		1. If a password manager is provided by your employer, use that account
		2. If you do not have a password manager provided to you, you can use tools such as 1Password, LastPass, or Bitwarden
		3. It is ok to write down a password, as long as you store that list somewhere secure such as a locked desk drawer. You do not want to carry that list in the same place that you carry your device.
		4. Never share your User ID or password with other users. Every individual user should have their own login credentials.
2. Phishing Emails
	1. Review sender name, is this someone they know? If not, look for the following signs:
		1. Does the email address match the sender’s name?
		2. If presented as a business/professional email, is the email address actually from a free account such as Gmail or Hotmail?
		3. Is the email address misspelled (for example, googel.com instead of google.com)?
		4. What time was the email sent? (An email from an executive in your office would likely not be sent at 3:00am.)
		5. HOT TIP: when on a mobile device, it can be difficult to see the entire address. It you receive a message and the email isn’t from a person directly (ie claiming to be Microsoft asking to change your password), expand the window so you can read their full email address.
	2. Does the email have an “External” warning or other system warning that the sender might not be who they say they are? If so, follow the above precautions
	3. Check the body of the email - TIP: slow down, count to three, and think before clicking.
		1. Hover over links to see if the website you’ll connect to matches what it says in the visible text
		2. Do links have odd domains, such as queenbee.exs or tuttle.e.zo
		3. ONLY open attachments if they are from someone you know (and you’ve confirmed it’s them by looking at the email address). But still be cautious if they end in .exe or .zip
		4. Is there a sense of urgency, something must be done now?
		5. Look for grammatical or spelling errors
		6. If you click a link, check the legitimacy of a website by looking for the HTTPS protocol in the address bar and by looking for the company's or organization's official website
		7. Be suspicious of emails that ask for personal information or financial credentials
	4. Report a suspicious email
		1. Use the report spam tool within your email platform
		2. If you don’t know where to find that tool, ask your Supervisor for help
3. Safely handling data
	1. Know how your organization classifies data and what each level means (public, internal, confidential, etc.)
		1. Follow prescribed procedures for each data level
	2. Follow the best practices when handling or sharing sensitive information such as birthdays, social security numbers, credit cards, and bank account numbers, whether it belongs to you or others
		1. Only share information with those who need to know
		2. Use email encryption or other secure tools for sending sensitive information. If you don’t know how to do that, ask your supervisor
		3. Know your surroundings when in a public space and limit discussion and visibility of sensitive data
		4. Do not transfer work-related data to your personal accounts
	3. Always backup data as requested by your organization. When available, use the backup functionality on your mobile device.
	4. When leaving your workstation, lock your device screen
	5. Only allow authorized personnel into secure spaces - it’s okay to not hold the door open and request that everyone authenticate with their security badge!
4. Avoiding device theft
	1. Enable all security measures such as a device password and location
		1. Never turn off or uninstall security tools
	2. Never leave your device unattended, even for a short period of time
	3. Report your lost device immediately
		1. Know whom in your organization should be notified
5. Removable Media
	1. Password protect any removable media
	2. Use only authorized removable media
	3. Virus scan any removable media
	4. Report lost removable media ASAP
6. Vishing
	1. Do not respond to unknown numbers
	2. Do not respond to suspicious calls
	3. Do not respond to prompts or buttons from unknown or suspicious calls
	4. Try to identify the caller's identity when possible
		1. Contact the organization associated with the caller
		2. Do not call a number provided by the caller, search the organization's number from a recognized source
	5. Do not provide any PII, divulge any passwords, login information, or credit card numbers
	6. Block automated calls or unknown numbers
7. Internet Browsing and Downloads
	1. Only download from secure or reputable websites
		1. Identify the legitimacy of the website using https or comparing the site to results on a search engine
	2. Scan files for viruses before downloading
		1. Pay attention to executable file extensions such as .exe or .scr
	3. Backup your documents
	4. In the event of downloading malicious software onto your computer
		1. Reset or restart your computer and restore your backup to prevent access to your files or documents
		2. Change your password immediately
	5. Be careful about what extensions you install. Browser extensions can be useful, but they can also be used to track your browsing activity or install malware on your device. Only install extensions from trusted sources.
	6. Use a privacy-focused search engine. A privacy-focused search engine, such as DuckDuckGo, will not track your search activity.
	7. Use a content blocker. A content blocker can help to block ads, trackers, and other malicious content.
	8. Limit cookies to only the “Strictly Necessary” category
8. Wifi
	1. Use only authorized devices or computers to connect to company wifi unless otherwise specifically allowed
	2. In general, do not use unsecured or free networks
		1. If the only option, use VPN
		2. Also, never send sensitive data over unsecured or free networks
	3. Ensure all devices or computers are password protected
		1. Passwords should be long and strong, with over 12 characters using a combination of uppercase, lowercase digits, numbers, and special characters
	4. Always update systems to latest version

Prerequisite Analysis and Prior Knowledge

1. Create a password
	1. Basic computer navigation
	2. How to change a password
2. Check for phishing email
	1. Familiarity with the body and heading of an email
	2. General understanding of how email works, including the email software
	3. General understanding of how email is used in a business setting
	4. General understanding of document identifiers, ie., .pdf, .exe, .zip
3. Data handling
	1. Basic computer navigation
	2. Know how to lock the computer
	3. Basic understanding of what constitutes sensitive data
4. Avoiding Device Theft
	1. How to password protect a device
	2. How to navigate through the settings of popular devices such as Iphone
5. Removal Media
	1. Familiarity with the types of media
	2. How to virus scan removable media
	3. How to password-protect removable media
6. Vishing
	1. How to identify a suspicious caller
	2. How to search organization websites on the internet
	3. Familiarity with information that should not be shared with a suspicious caller
7. Internet Downloads
	1. Understanding of what a reputable site looks like
	2. How to identify a secure website (Http vs. Https)
	3. How to back up data
	4. How to virus scan electronic files
8. Wifi
	1. How to set up long and strong passwords
	2. How to connect to a wireless network/Wifi
	3. How to use a company VPN

# Learning Requirements Analysis (LRA)

| **Work Situations** | **Could a Job Aid Be Appropriate?** | **Notes** |
| --- | --- | --- |
| **Consider Work Situations Where a Job Aid Could Be Appropriate. (check one)** |  |
| Sequence is critical for task success. | X Yes ◻ No ◻ Need to gather more information |
| A job aid could enhance performer confidence. | X Yes ◻ No ◻ Need to gather more information |
| The consequences of workplace error are high. | X Yes ◻ No ◻ Need to gather more information |
| The task is performed infrequently. | ◻ Yes ◻ No X Some of the tasks, such as changing a password |
| The task is easy to get wrong. | X Yes ◻ No ◻ Need to gather more information |
| Task performance depends on frequently changing information. | ◻ Yes X No ◻ Need to gather more information |
| Complex task performance can be described in detail. | X Yes ◻ No ◻ Need to gather more information |
| Task performance requires the use of a large body of information. | ◻ Yes X No ◻ Need to gather more information |
| **Consider Work Situations Where a Job Aid Could Be Inappropriate. (check one)** |
| Use of a job aid could damage credibility or customer confidence | ◻ Yes X No ◻ Need to gather more information |
| Use of a job aid would slow or degrade performance. | ◻ Yes X No ◻ Need to gather more information |
| The workplace environment doesn’t lend itself to a job aid. | ◻ Yes X No ◻ Need to gather more information |
| Performer memory is a better option. | ◻ Yes X No ◻ Need to gather more information |

## Training Configuration

| **What training configuration is appropriate to support the task? (check one)** | **Rationale for each configuration** |
| --- | --- |
| ▢ Informal learning | The task is not a priority for the organization. |
| ▢ Standalone job aids (no training) | The task is a priority, job aids are appropriate, and the task involves a simple skill. |
| X **Introductory training with job aids** | The task is a priority, job aids are appropriate, and the task involves either a* Relatively straightforward skill that requires demonstration.
* Simple skill where learners won't use the job aid on their own without a formal introduction and demonstration.
 |
| ▢ Extensive training with job aids | The task is a priority, job aids are appropriate, and the task involves a complex or difficult skill that requires demonstration, practice, coaching, and feedback. |
| ▢ Extensive training to memory | The task is a priority, job aids are not appropriate, and the task involves a complex or difficult skill that requires demonstration, practice, coaching, and feedback. |

#### Planned Configuration

Based on our analysis, we will complete the following:

* Introductory video to capture learner’s attention and create an emotional hook/WIIFM (Gagné et al., 2005) (Attitude)
* Leverage existing NCA video content for the educational content (Knowledge)
* Build a branching scenario to assess learner’s performance (Skills)
* Create a script to be used by organizational leader to introduce the lesson and gain buy-in from the learner (Attitude)
* Create a branded job aid that will support the learner as they complete the tasks (Knowledge and Skills)

#

# References

Gagné, R. M., Wager, W., Golas, K. C., Keller, J. M., & Russell, J. D. (2005). Principles of instructional design, 5th edition. *Performance Improvement*, *44*(2), 44–46. https://doi.org/10.1002/pfi.4140440211

Huisman, J. (n.d.). *KnowBe4’s 2022 Phishing By Industry Benchmarking Report Reveals that 32.4% of Untrained End Users Will Fail a Phishing Test*. <https://blog.knowbe4.com/knowbe4-2022-phishing-by-industry-benchmarking-report>

Tessian. (2022, March 29). *The Psychology of Human Error 2020 - Tessian*. https://www.tessian.com/research/the-psychology-of-human-error/