Please Note…

This webinar and the engagement tools will be recorded.

An archive will be available on the event website.

Federal Information Security Educators (FISSEA)

Summer Forum

August 23, 2023

1:00pm – 4:00pm ET

#FISSEA2023 | nist.gov/fissea

fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

FISSEA Welcoming Remarks

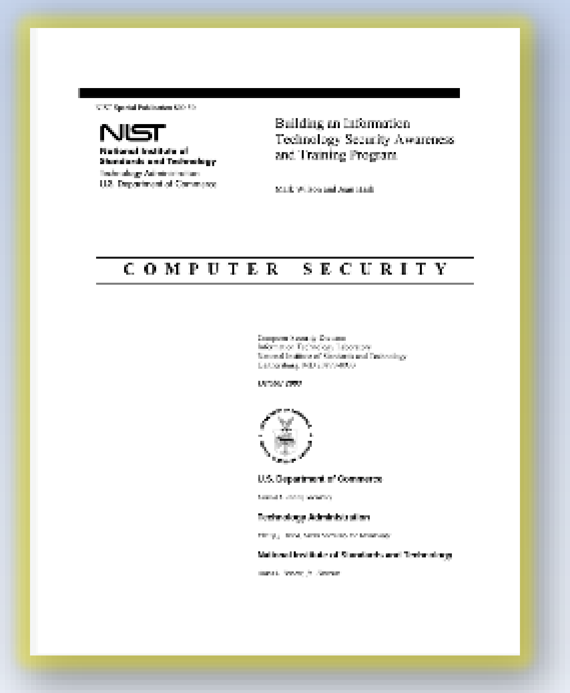
Marian Merritt

NICE Deputy Director
National Institute of Standards and Technology

NIST SP 800-50

- Building an Information Technology Security Awareness & Training Program - 2003 (20 years ago)
- Revision draft will be public in September
- Co-authoring team from several Federal agencies

- Goals:
  - Leverage NIST guidance
  - Develop consistent language
  - Reflect research from FISSEA community
  - Address challenges such as measuring impact



NIST Special Publication 800-50

NIST
National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

Building an Information
Technology Security Awareness
and Training Program

Mark Wilson and Joan Hash

COMPUTER SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8933

October 2003

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

NIST SP 800-50, continued

- “Building a Cybersecurity and Privacy Learning Program”
- The learning program supports a culture of respect for employees
- Everyone plays some type of role in managing the organization’s cybersecurity and privacy risk
- Includes privacy as a significant component
- The learning program is a cyclical, iterative model
- Consolidates 800-16, incorporates NICE Framework
- Intended to be collaborative, flexible, scalable

- **We look forward to your comments!**

Welcome and Event Logistics

Kendra Henthorne

FISSEA Co-Chair

fissea FEDERAL CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

#FISSEA2023

Get Involved

Subscribe to the FISSEA Mailing List
FISSEAUpdates@list.nist.gov

Volunteer for the Planning Committee

Serve on the Contest or Award Committees for 2024
Email fissea@list.nist.gov

Submit a presentation proposal for a future FISSEA Forum
https://www.surveymonkey.com/r/fisseacallforpresentations

fissea FEDERAL CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

#FISSEA2023

Opening Keynote

AI: Where We're Going and How (Not?) to Get There

Anthony Boese

Interagency Programs Manager and Ethics Officer
National Artificial Intelligence Institute
United States Department of Veterans Affairs

fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

#FISSEA2023

National Artificial Intelligence Institute

AI: Where We're Going and How (Not?) to Get There

Anthony Boese, MA, MPP
Interagency Programs Manager
Presidential Management Fellow
VA National Artificial Intelligence Institute (NAII)

The Promise of AI

Three Tier-one Added Values from AI

Increased Efficiency

- Currently, AI is deployed in many sectors to do simple, repetitive tasks more quickly and with less investment/energy
- Soon, increases in robotics integration and spatial and linguistic awareness will extend the diversity and quality of AI-led tasks

Unreal Time to Spend

- Especially relative to a human, AI's can perform thousands of times the considerations/ calculations without rest
- The ability to consider myriad counterfactuals could make AI decision making more reliable and better hypo-tested than human decision making

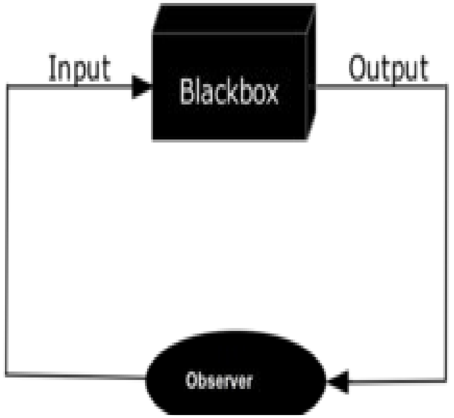
The Rational Machine

- In theory, an AI could and should be a rational, neutral, and informed director and/or arbiter of policy and action
- This might be untenable, but would pose the highest value if achieved

National Artificial Intelligence Institute

The Direct Risks of AI

When AI Crosses the Line



Opaque Bias

- A critical and perhaps inescapable concern with AI is bias – in the training data, sample data, data gathering, modeling, and/or the circumstances under which each of these are generated/occur

Unaligned Values

- What the AI values is not per se what we value
- We *could* code and model to avoid this, but
- Humans have little consistency in what they value and, more importantly, how they communicate those valuations

Human-less Loops

- This is a deployment concern more than something about the AI itself
- Here, the concern is both epistemic and meta/physical

The Downstream Risks of AI

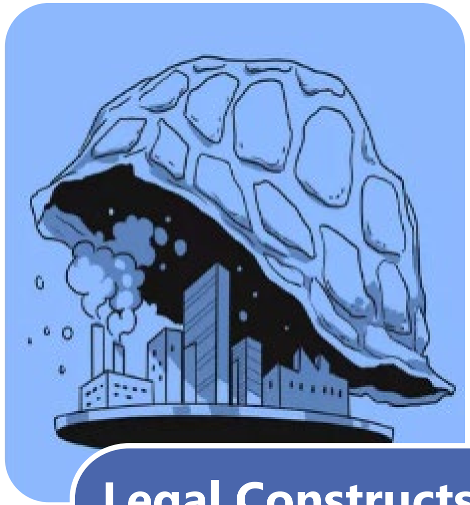
When AI is Part of the Chain

Inequity Compounding

- Those with the means to acquire further/better means to production, especially when they can do so more quickly, are near-guaranteed economic supremacy

Environmental Impact

- Alike Crypto: White House Fact Sheet reports 140 ± 30 million metric tons of carbon dioxide per year
- For AI: MIT reported that training just one AI model can emit more than 626,000lbs of CO2 – nearly five times the lifetime emissions of an average American car.



Legal Constructs; Shells

- Causality and Agency regarding AI as independent (or not) of their creators and/or handlers remains unsettled
- AI personhood remains unsettled

Methods for Mitigation

Vanguard Mitigations

Educated Users

- No matter how well designed or secured, underinformed and undertrained users are the greatest liability

Sys/SBOMS

- In this case, embrace the fallacy of genesis
- Though, domestic might not mean good
- Nevertheless, know whence comes your AI

Trustworthy AI Principles

- EO 13960 and EO 14091
- Agency-level Frameworks
- International Frameworks
- Private Sector Efforts

Next-stage Mitigations

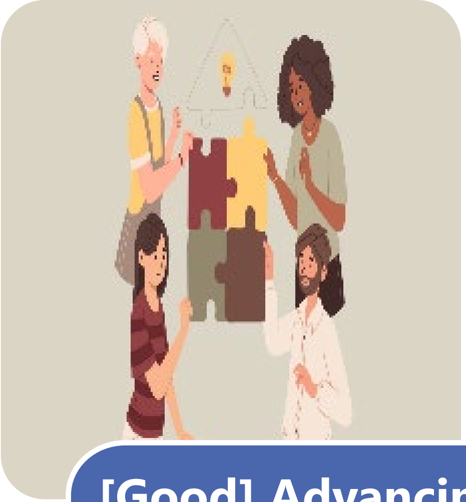
National Artificial Intelligence Institute

TAI Consistency

- Interagency Crosswalks
- Public/Private Crosswalks
- International Crosswalks

Oversight and Tracking

- Humans in the loop
- Policy-first and strategy-backed deployment and expansion
- Transparent reporting to stakeholders and regulators
- No black-box AIs



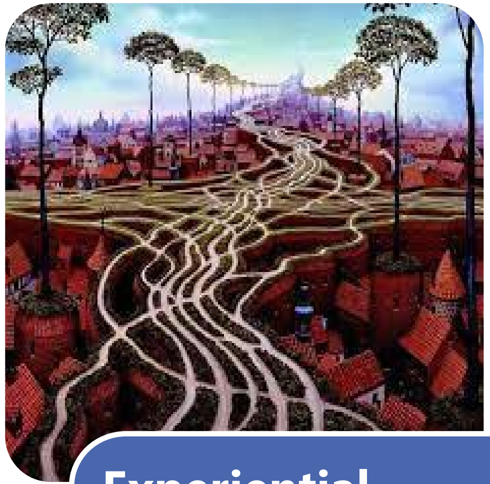
[Good] Advancing AI

- Privacy Advancing
- Equity Advancing
- Security Advancing
- Peace Advancing
- Etc.

On Diversity

Demographic

- To mean race, gender, age, income bracket, living arrangement, etc.
- Leverage Strategic Partnerships



Experiential

- Some overlap with demographic but also what jobs you’ve had, education you’ve undertaken, places you’ve lived, etc.
- Leverage Strategic Partnerships

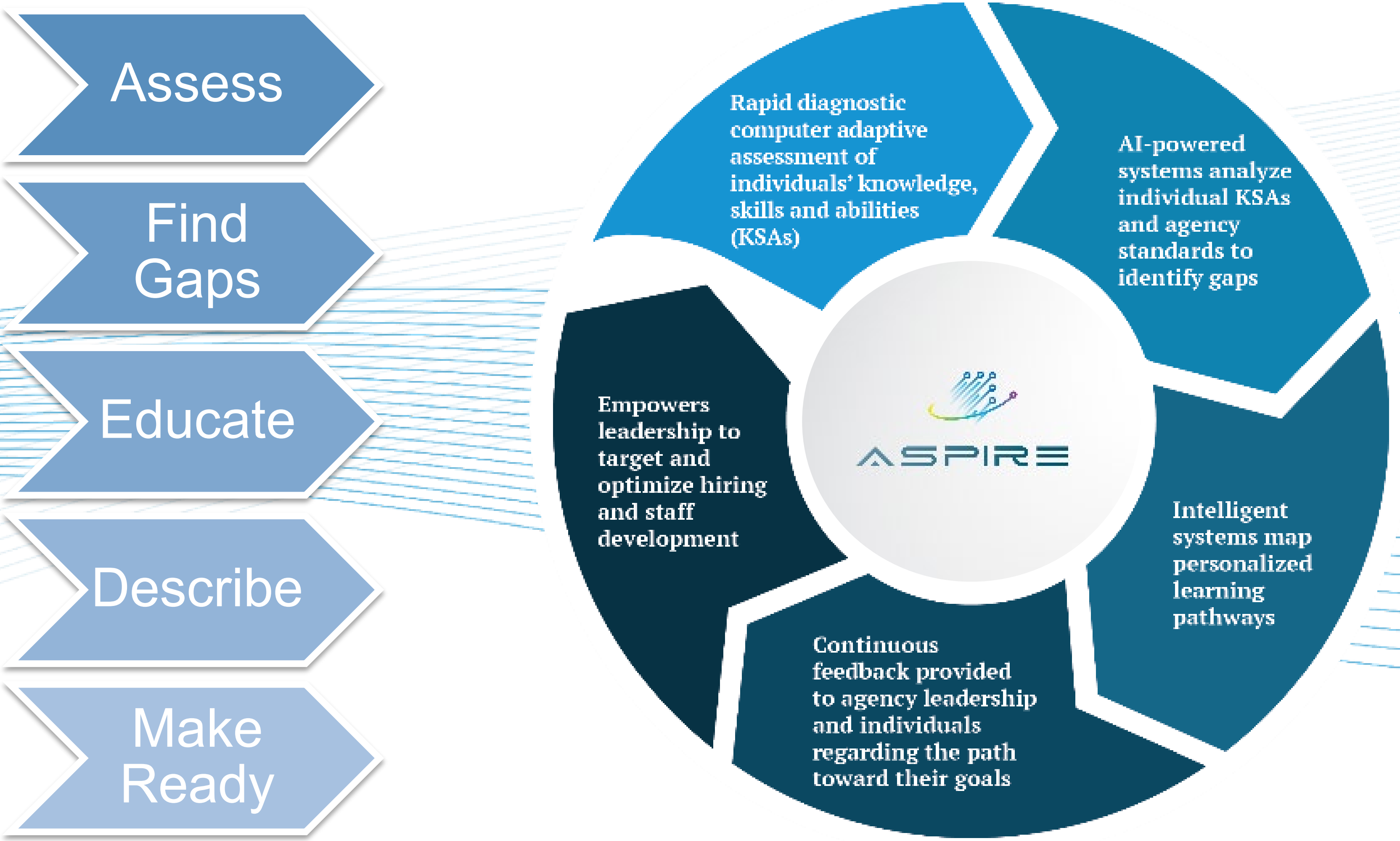
Expertival

- Proper AI and AI policy development needs tech folks, social science folks, humanities folks, legal experts, and context-relevant experts (e.g., doctors, service members, etc.)
- Leverage Strategic Partnerships

Use Case: ASPIRE

All Services Personnel and Readiness Engine

National Artificial Intelligence Institute



Rapid diagnostic computer adaptive assessment of individuals' knowledge, skills and abilities (KSAs)

AI-powered systems analyze individual KSAs and agency standards to identify gaps

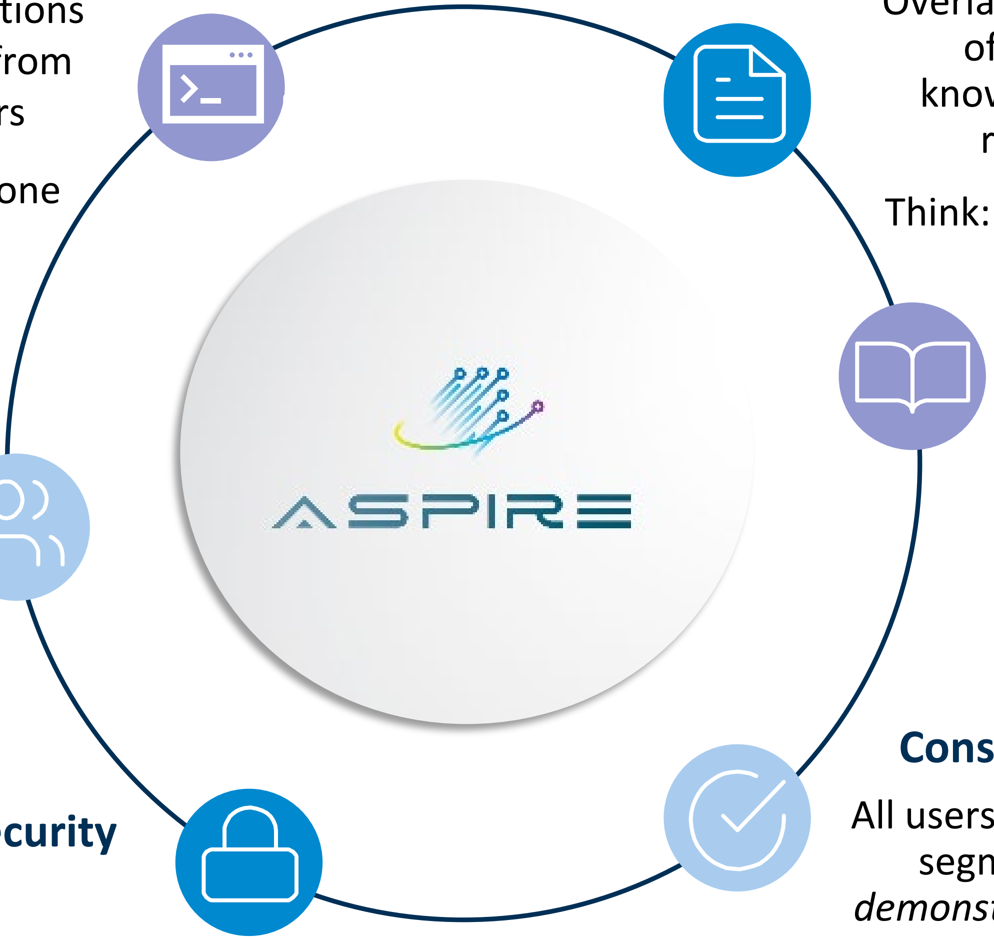
Intelligent systems map personalized learning pathways

Continuous feedback provided to agency leadership and individuals regarding the path toward their goals

Empowers leadership to target and optimize hiring and staff development

ASPIRE PARTNERS

DEPARTMENT OF VETERANS AFFAIRS · UNITED STATES OF AMERICA
DEPARTMENT OF THE NAVY · UNITED STATES OF AMERICA
DEPARTMENT OF THE AIR FORCE · UNITED STATES OF AMERICA · MCMXLVII
NASA
DEPARTMENT OF LABOR · UNITED STATES OF AMERICA
DEPARTMENT OF HEALTH & HUMAN SERVICES · USA



Consistent Language

Overlapping definitions of competencies from uniform masters

Think: Rosetta Stone

Consistent Predications

Overlapping descriptions of role and rate knowledge and skills requirements

Think: Animal Taxonomy

Consistent Audit

Humans in the loop

Automated auditing and improvement

Consistent Education

Uniform yet diverse, expansive, and accessible learning content

Think: Common Core

Consistent Security

SBOM

IL5 planned

PHI/PII Standards

Consistent Validation

All users after any education segment will have to *demonstrate* the knowledge gained

Think: Driving Test

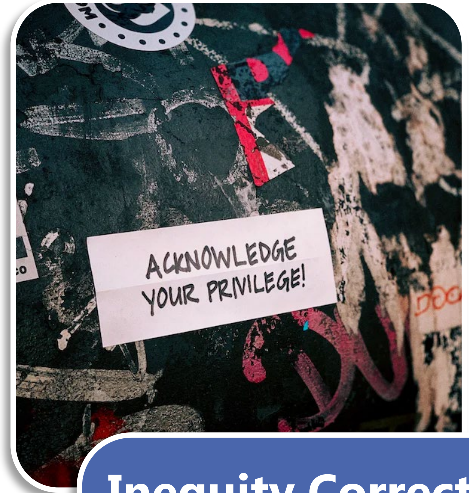
Equity and Security

Security

- Identity-tied data doesn’t move
- Messaging Layer Security
- Capsulations for austere environments
- Binary-level S/SysBOM

Equity Advancing

- All are reviewed on equal, impartial footing
- Designed by a diverse and multifaceted team
- Consistently audited for biases
- Accessibility as a priority



Inequity Correcting

- Any comer can prove themselves despite lack of past opportunity to garner credentials
- Any comer can be challenged to validate and verify their credentials

Thank you!

Questions?

E-mail: Anthony.boese@va.gov

Privacy and Ethics as a Foundation for AI Risk Management Training

Julie McEwen

Privacy Capability Area Lead, Principal Cybersecurity & Privacy Engineer
MITRE

fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

#FISSEA2023

Privacy and Ethics as a Foundation for AI Risk Management Training

Federal Information Security Educators (FISSEA) Summer Forum

Julie McEwen, CISSP, PMP, FIP, CIPP/G, CIPP/US, CIPM, CIPT

23 August 2023

Agenda

- The Basics
    - What is artificial intelligence (AI)?
    - What is privacy?
        - What are the Fair Information Practice Principles?
- AI Risks and Privacy
    - Privacy risks for AI use
    - NIST AI Risk Management Framework
    - AI governance and privacy
    - Privacy-enhanced AI: Governance
    - Privacy-enhanced AI: Privacy engineering
- Recommendations
- Resources
- Questions

The Basics

What is Artificial Intelligence (AI)?

- Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
- An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.

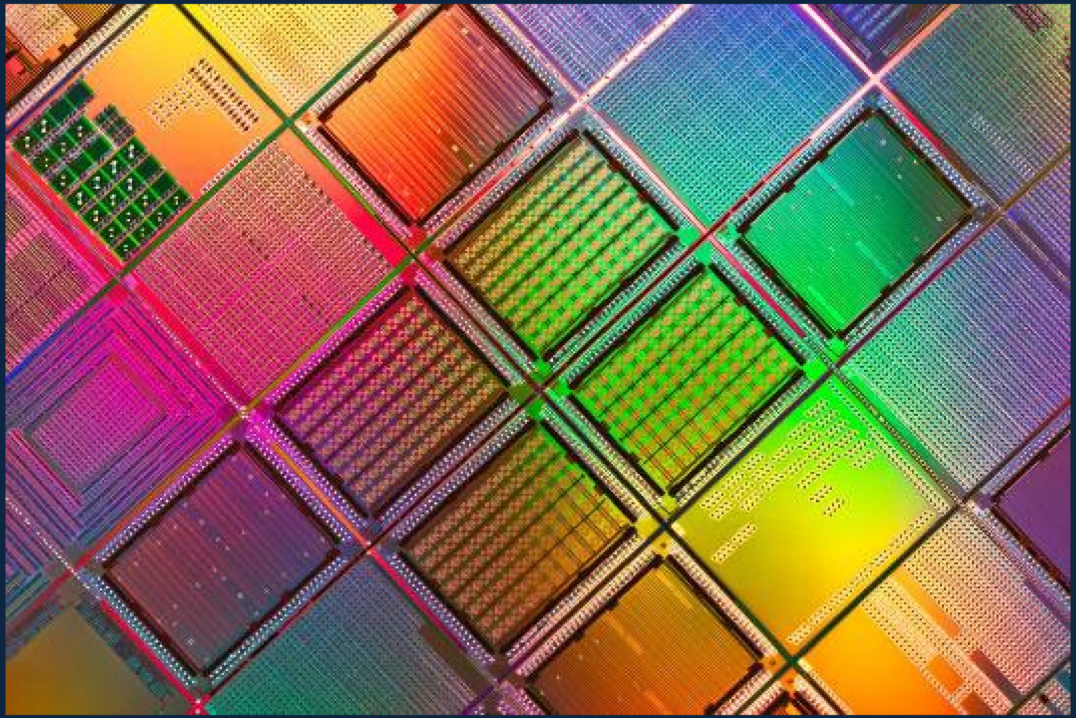


Image Source: MITRE

Definition Source: John S. McCain National Defense Authorization Act for Fiscal Year 2019, P.L. 115-232, Sec. 1051, https://www.nscai.gov/about/authorization-act/

MITRE

What is Privacy?

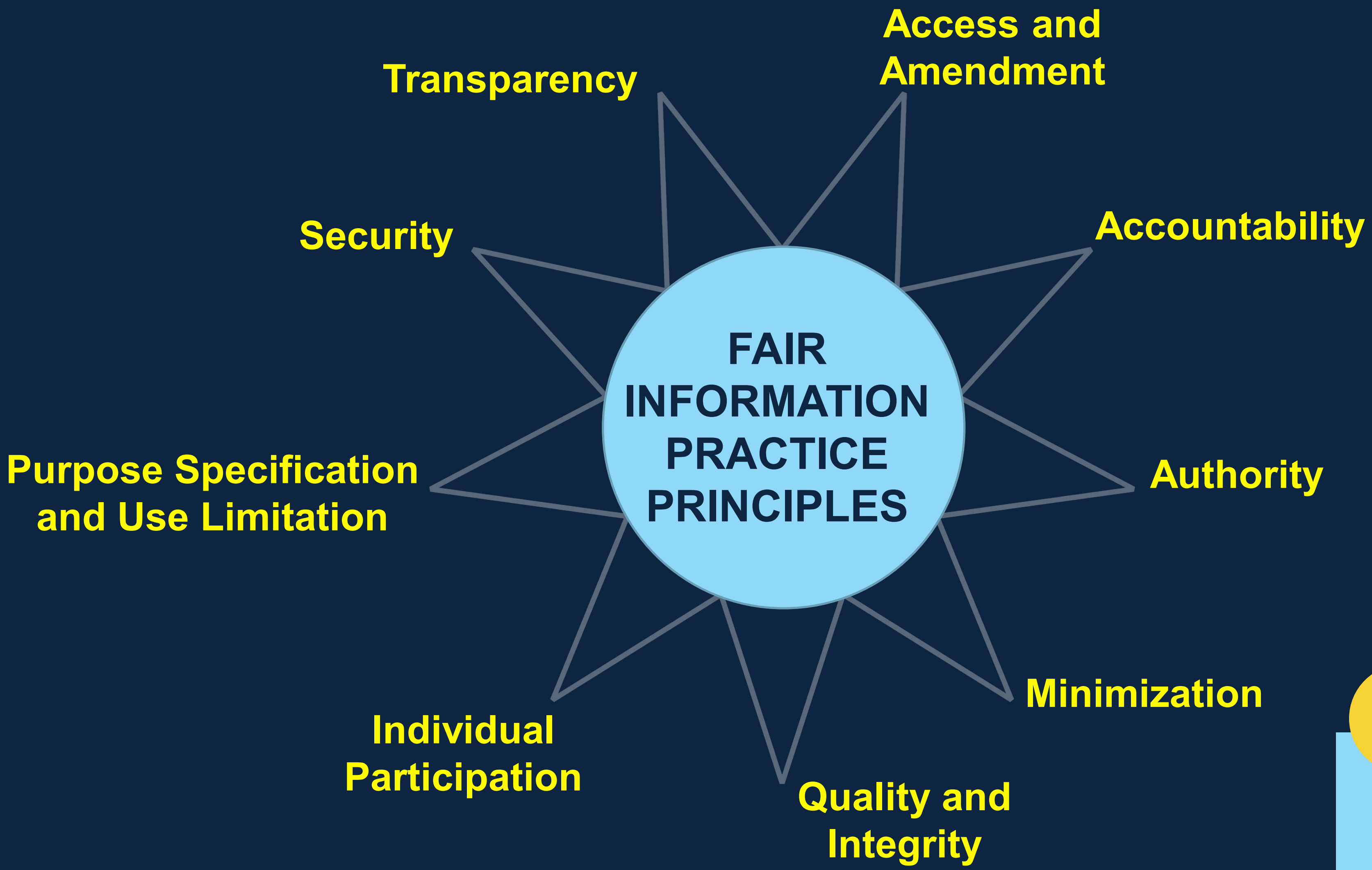
The ability of individuals to exercise control over the collection, use, and dissemination of their Personally Identifiable Information (PII).

A fundamental right to be secure in one's person, house, papers, and effects (extends to speech, beliefs, and associations) (US Constitution, First and Fourth Amendments)

Data Protection (European Union Approach – Comprehensive): Lawful restrictions placed on entities that process personal information

Image Source: MITRE

What are the Fair Information Practice Principles (FIPPs)*?



FAIR INFORMATION PRACTICE PRINCIPLES

Access and Amendment

Accountability

Authority

Minimization

Quality and Integrity

Individual Participation

Purpose Specification and Use Limitation

Security

Transparency

In **some environments** (e.g., law enforcement and intelligence), opportunities for **access** and amendment and individual participation are often **extremely limited**

*Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource, Appendix II, Responsibilities for Managing Personally Identifiable Information, July 28, 2016

AI Risks and Privacy

Privacy Risks for AI Use

- Increased difficulty in protecting or screening out personal data
- Increased difficulty in deidentifying data within datasets
- Increased possibilities for reidentifying individuals based on comparing data across deidentified data sets
- Appropriation of personal information for model training
- Allowing inference to identify individuals
- Lack of transparency of use
- Bias and fairness
  - Protected classes and other groups
- Inaccurate models

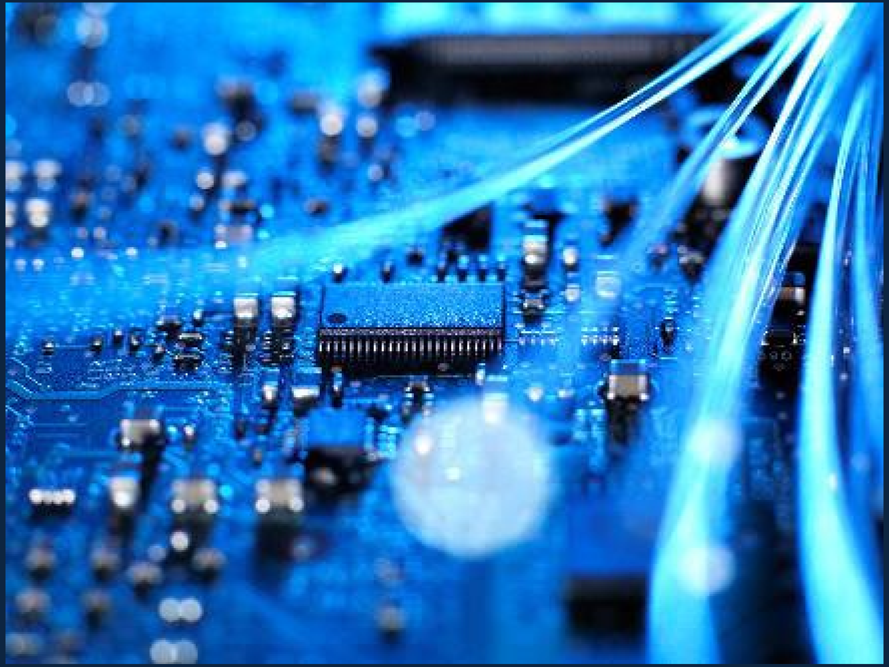
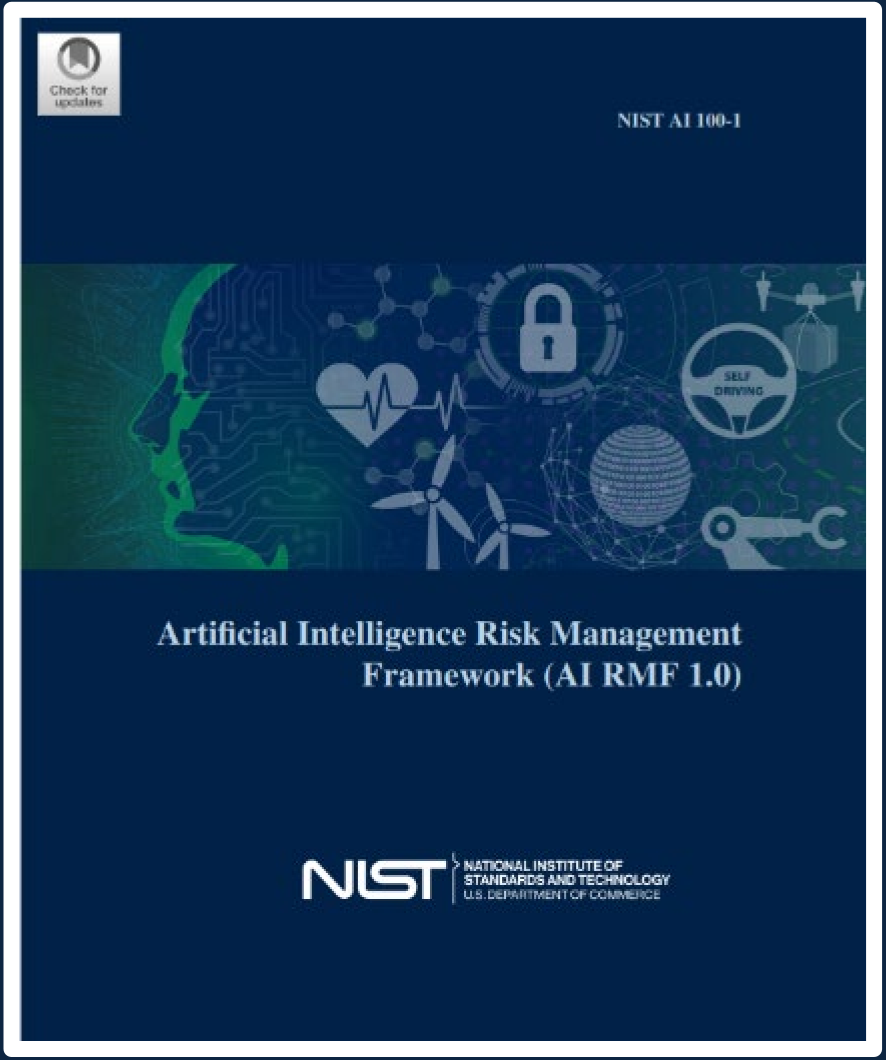


Image Source: MITRE

MITRE

NIST AI Risk Management Framework

- Characteristics of trustworthy AI systems include being:
  - Valid and reliable
  - Safe
  - Secure and resilient
  - Accountable and transparent
  - Explainable and interpretable
  - Privacy enhanced
  - Fair with their harmful biases managed


Check for updates

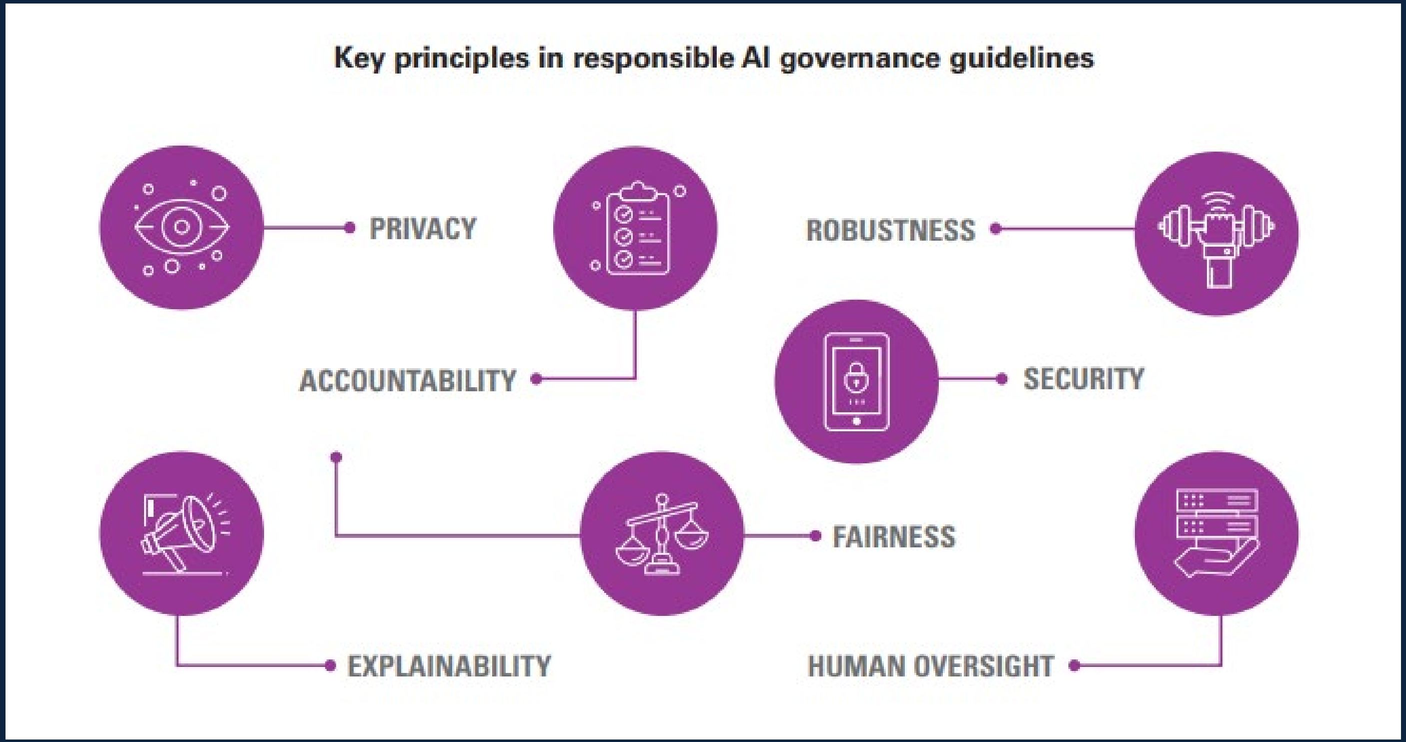
NIST AI 100-1

Artificial Intelligence Risk Management Framework (AI RMF 1.0)

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

AI Governance and Privacy

- IAPP Privacy and AI Governance Report findings
  - AI and privacy overlap in several key areas
    - Explainability
    - Fairness
    - Security
    - Accountability
  - Collaboration between AI governance and privacy governance



Key principles in responsible AI governance guidelines

Image Source: IAPP Privacy and AI Governance Report Executive Summary, January 2023

MITRE

Privacy-Enhanced AI: Governance

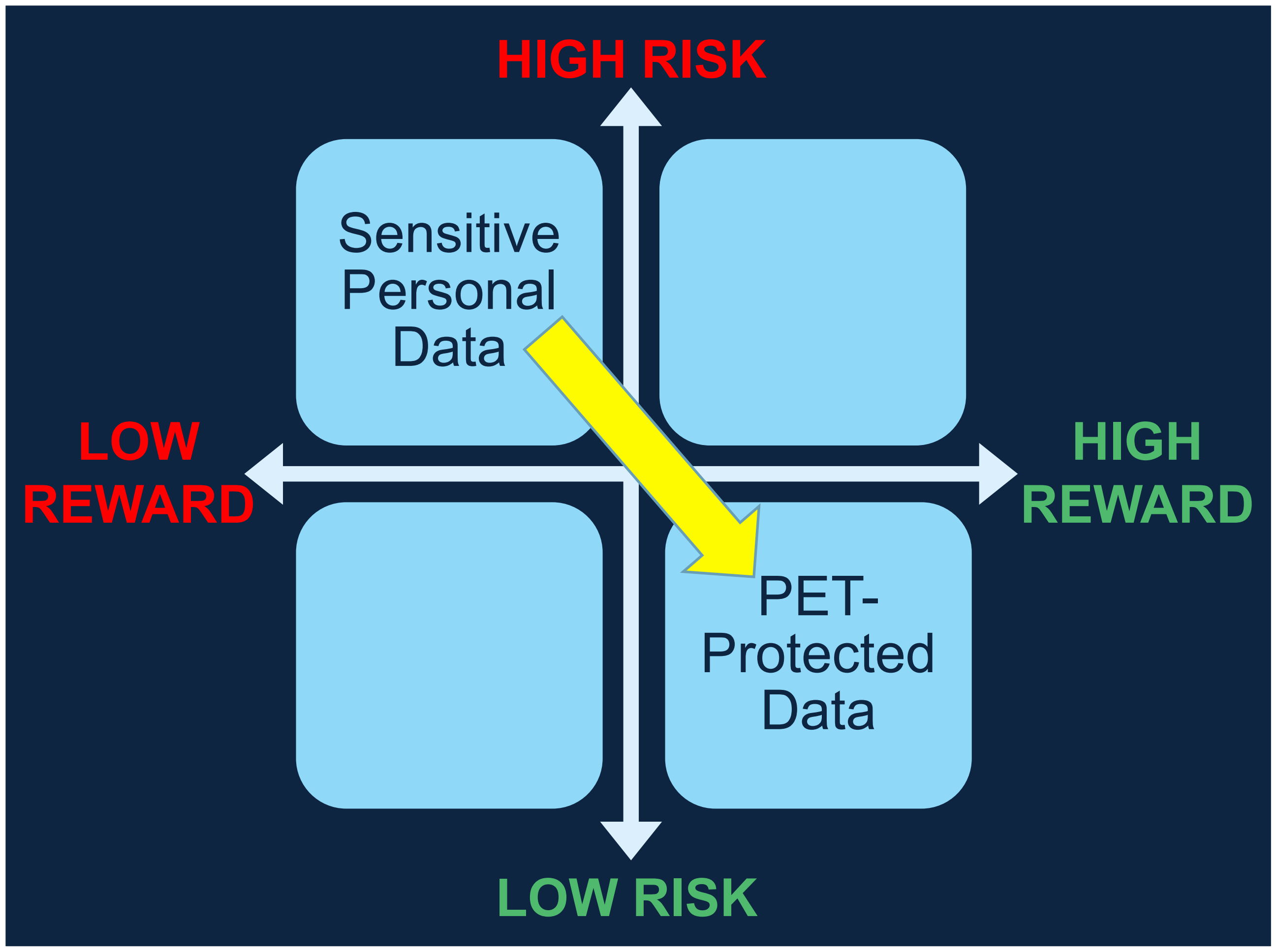
- Establish AI governance including data governance and privacy
  - AI Governance by Design: Build governance in from the beginning and throughout the lifecycle
  - Think about legal and ethical socio-technical issues early with diverse teams during ideation/planning phase
  - Build AI governance on existing privacy and data security governance policies and procedures

Image Source: MITRE

MITRE

Privacy-Enhanced AI: Privacy Engineering

- Privacy by Design
  - Privacy must be built into AI systems from the beginning.
- Privacy engineering implements the concept of Privacy by Design
- Privacy design approaches
  - Data minimization
  - Data tagging
  - Data de-identification / anonymization / pseudonymization
- Use of Privacy-Enhancing Technologies (PETs)



Risk Reduction Via Use of PETs

MITRE

Recommendations

- Practice AI Governance by Design by building governance in from the beginning and throughout the lifecycle
- Build AI governance on existing privacy and data security governance policies and procedures
- Discuss AI privacy risks and harms, including potential bias and discrimination, in risk management training
- Enhance knowledge of privacy engineering in concert with AI risk management training
- Update risk management training regularly to reflect changes in AI technology, uses, and implementation approaches

Resources

- Executive Order 13960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, December 3, 2020, https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government
- EU Artificial Intelligence Act, https://artificialintelligenceact.eu
- EU-US Trade and Technology Council (TTC) Joint Roadmap on Evaluation and Measurement Tools for Trustworthy AI and Risk Management, https://digital-strategy.ec.europa.eu/en/library/ttc-joint-roadmap-trustworthy-ai-and-risk-management
- International Association of Privacy Professionals (IAPP) Privacy and AI Governance Report (Summary), https://iapp.org/resources/article/ai-governance-report-summary/
- National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework (AI RMF 1.0), https://www.nist.gov/itl/ai-risk-management-framework
- National Security Commission on Artificial Intelligence (NSCAI) Final Report, https://www.nscai.gov/2021-final-report/
- US White House Blueprint for an AI Bill of Rights, https://www.whitehouse.gov/ostp/ai-bill-of-rights/

Questions?

Julie McEwen, Privacy Capability Lead, MITRE Corporation

jmcewen@mitre.org

MITRE

Federal Information Security Educators (FISSEA) Summer Forum

BREAK

The Forum will resume at 2:30pm EDT

#FISSEA2023 | nist.gov/fissea

Welcome Back!

Menachem Goldstein

FISSEA Co-Chair

Phishing for User Context: Understanding the NIST Phish Scale

Dr. Shanée Dawkins

Computer Scientist
National Institute of Standards and Technology

fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

#FISSEA2023

Phishing for User Context: Understanding the NIST Phish Scale

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Shanée Dawkins, Ph.D.
Jody Jacobs, M.S.

August 2023

Disclaimer

Throughout the presentation, certain commercial companies or products may be identified to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the companies or products identified are necessarily the best available for the purpose.

Presentation Overview

- Who we are
- Phishing threat landscape
- Our research & the NIST Phish Scale

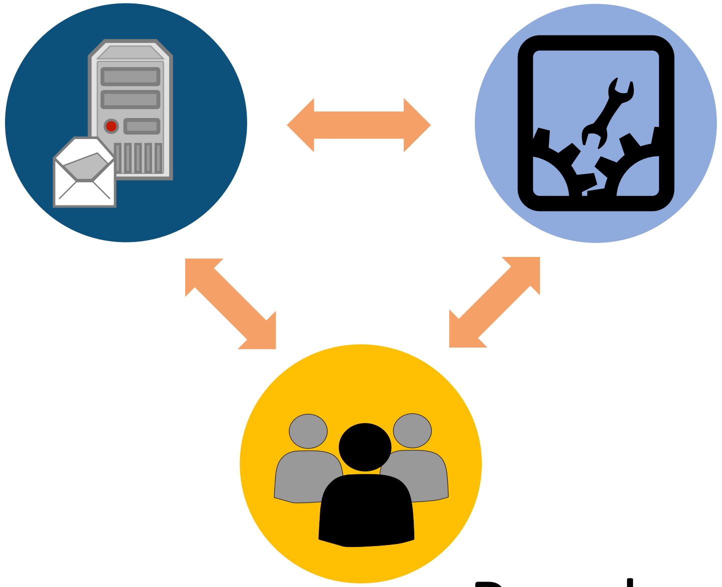
Championing the Human in I.T.

Phishing Threat Landscape

Phishing Landscape

⬆ 5x	Phishing attacks have quintupled since 2020.[1]
$10.2B	Victim losses in 2022.[2]
82%	Breaches involved the human element in 2021.[3]
74%	Reported spear phishing attacks in 2022.[4]

Phishing Defense



Technology

- Filtering
- DMARC, DKIM
- AI & ML
- Multi-factor authentication

Process

- Identify vulnerabilities
- Limiting publicly available information
- Awareness training
- Easy and clear reporting mechanism
- Meaningful metrics

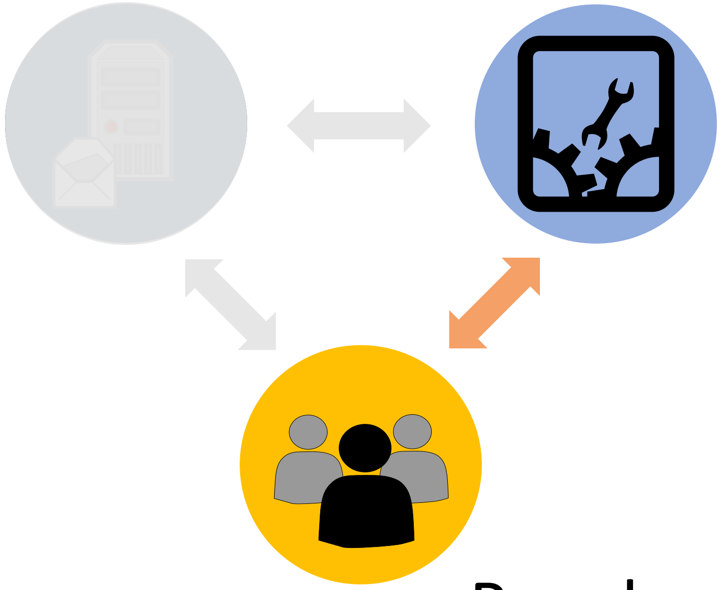
People

- End users
- IT security staff
- Leadership

Phishing Defense

Technology

- Filtering
- DMARC, DKIM
- AI & ML
- Multi-factor authentication



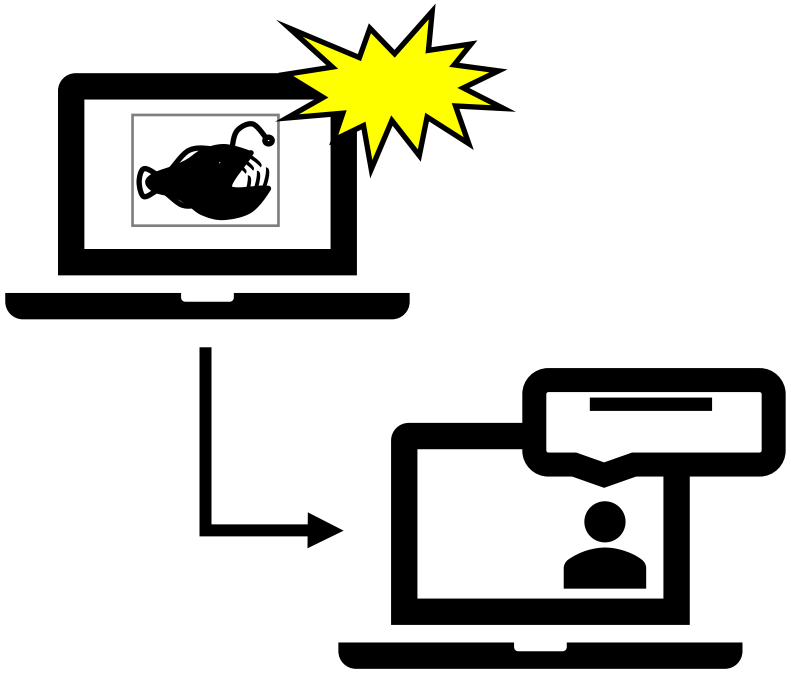
Process

- Identify vulnerabilities
- Limiting publicly available information
- Awareness training
- Easy and clear reporting mechanism
- Meaningful metrics

People

- End users
- IT security staff
- Leadership

Phishing Awareness Training



Training in Practice

- Simulated phishing emails
- Gamify phishing
  - e.g., phish hunting badges, shark awards
- Staff Profiles

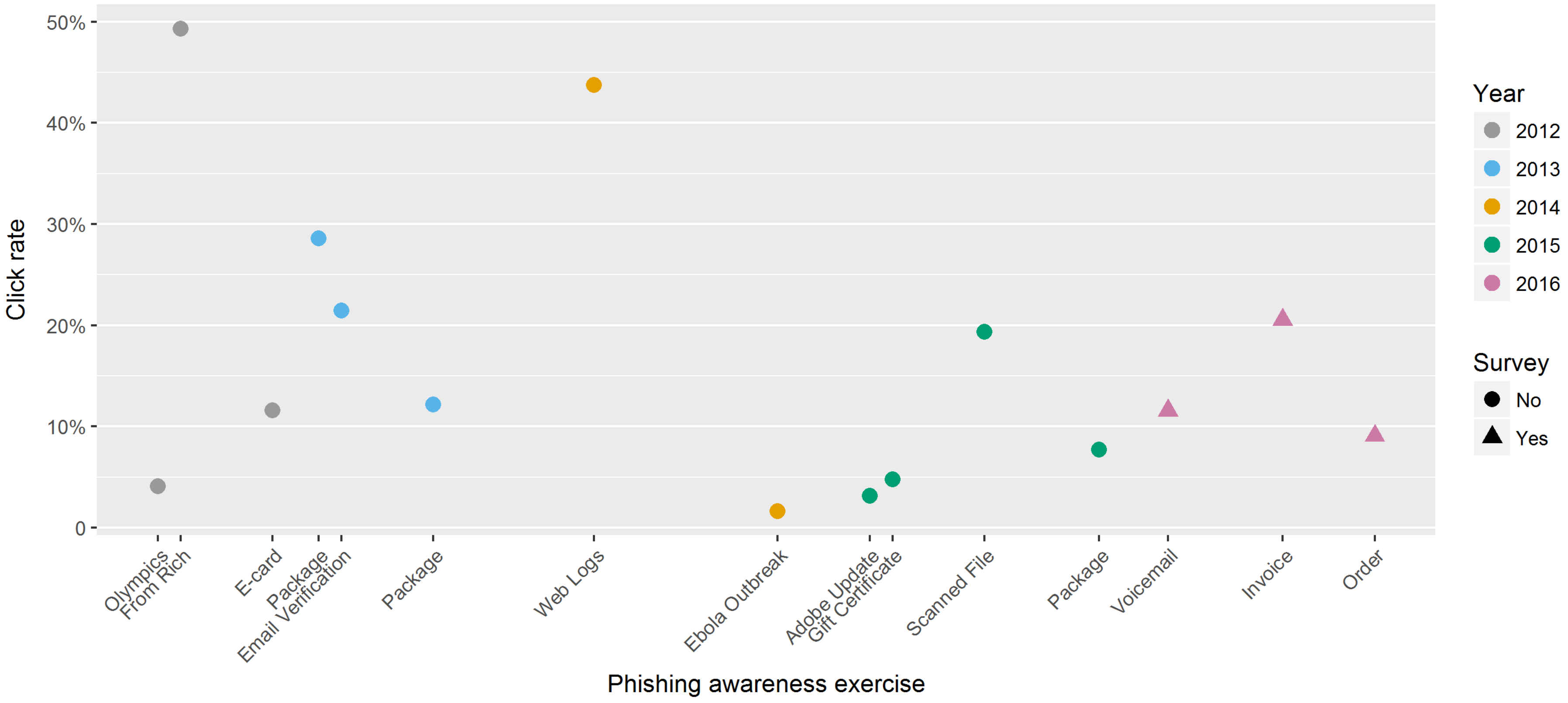
Common Metrics and Behaviors

- Click rates
- Reporting rates
- Repeat clickers
- Protective stewards[5]

Our Research

Our Research – Phishing Awareness Study

- 15 training exercises over 4.5 years



Our Research – Phishing Awareness Study

49.3%

3.2%

4.8%

11.0%

8.7%

9.1%

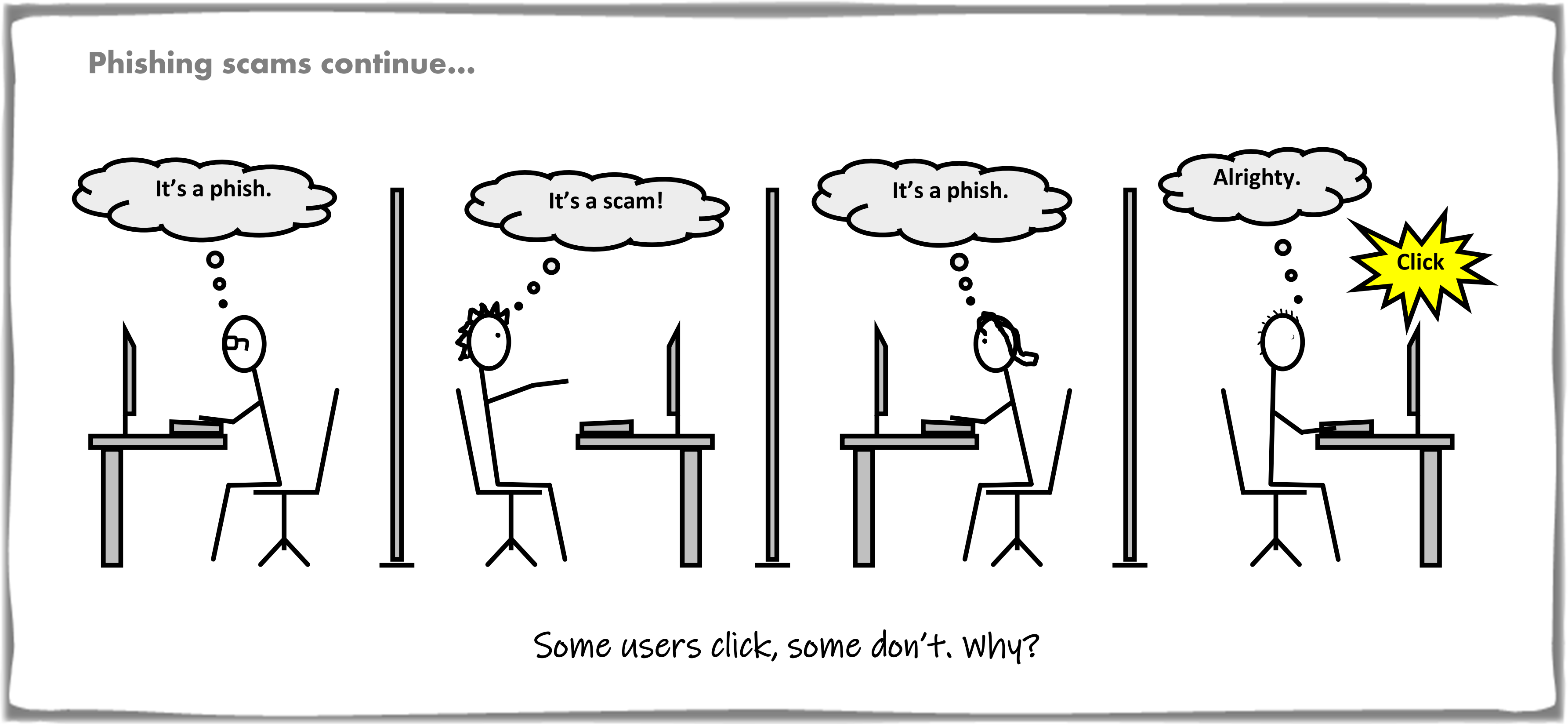
43.8%

11.6%

20.5%

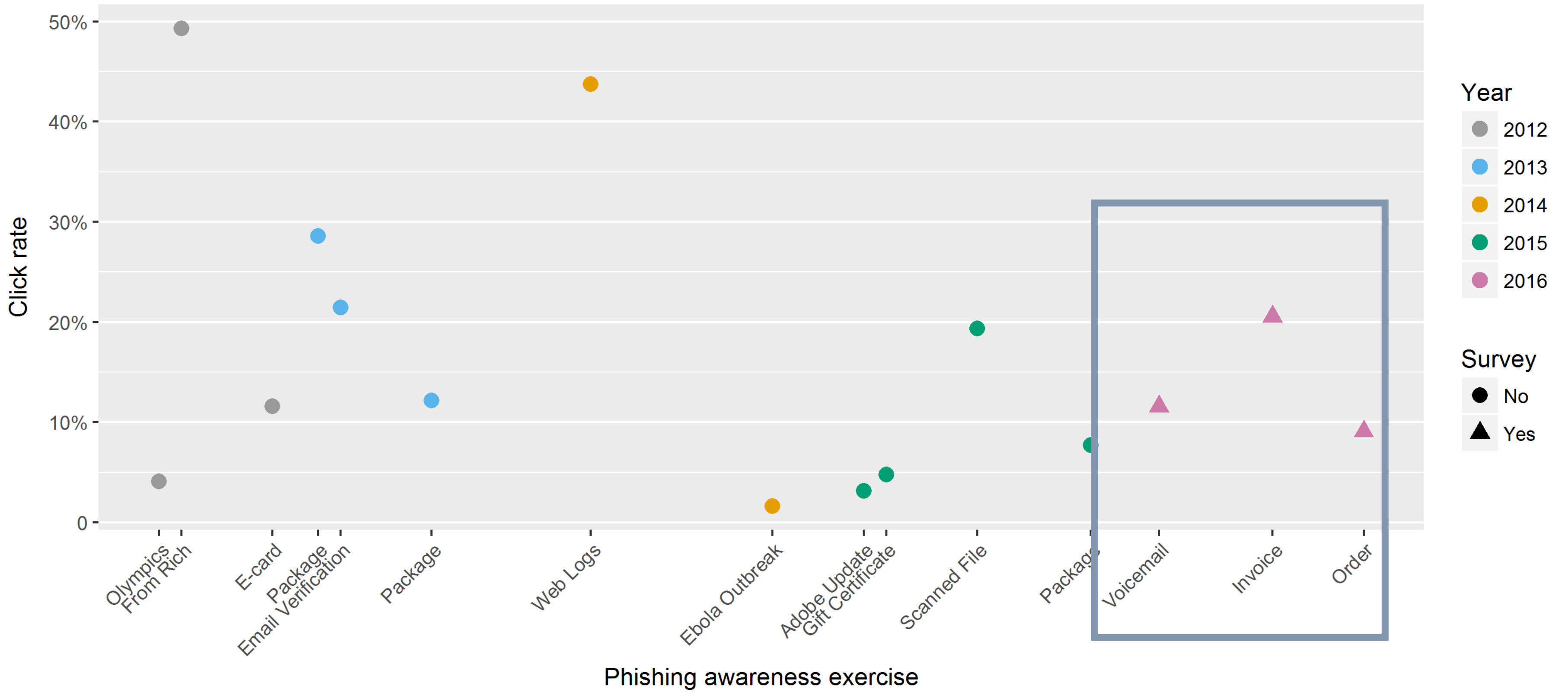
19.4%

Our Research – Phishing Awareness Study


Phishing scams continue...
It's a phish.
It's a scam!
It's a phish.
Alrighty.
Click
Some users click, some don't. Why?

Our Research – Phishing Awareness Study

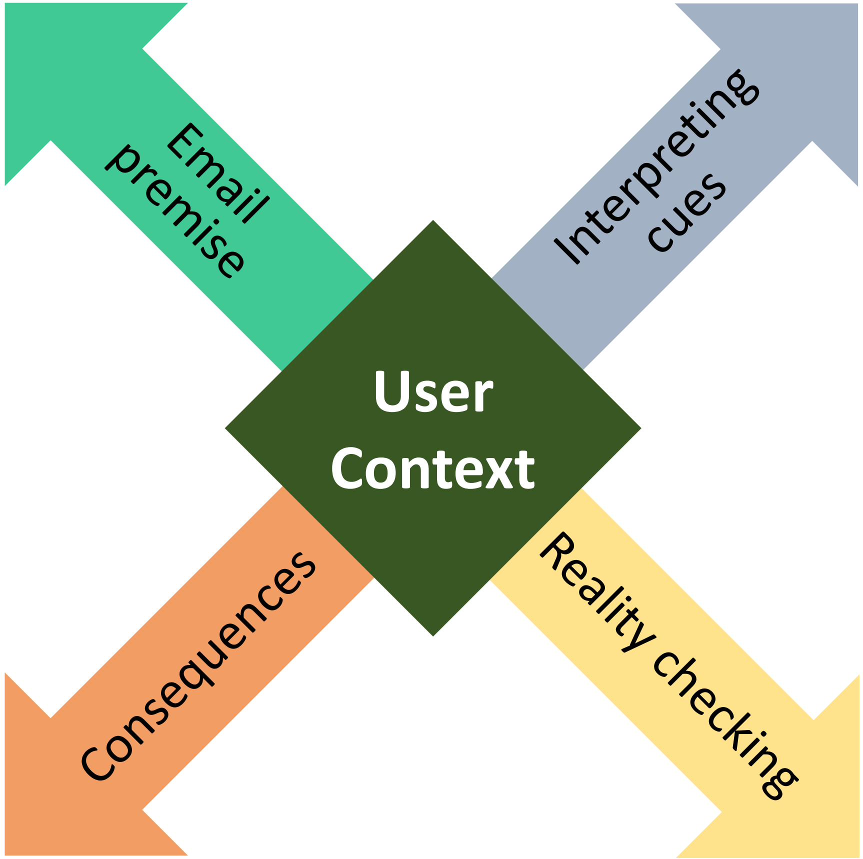
- 15 training exercises over 4.5 years
- Corresponding survey data for last 3 exercises



Our Research – Phishing Awareness Study

Alignment vs. misalignment with expectations and external events

Compelling vs. suspicious cues



Concern over consequences

Reality-checking strategies

Our Research – NIST Phish Scale

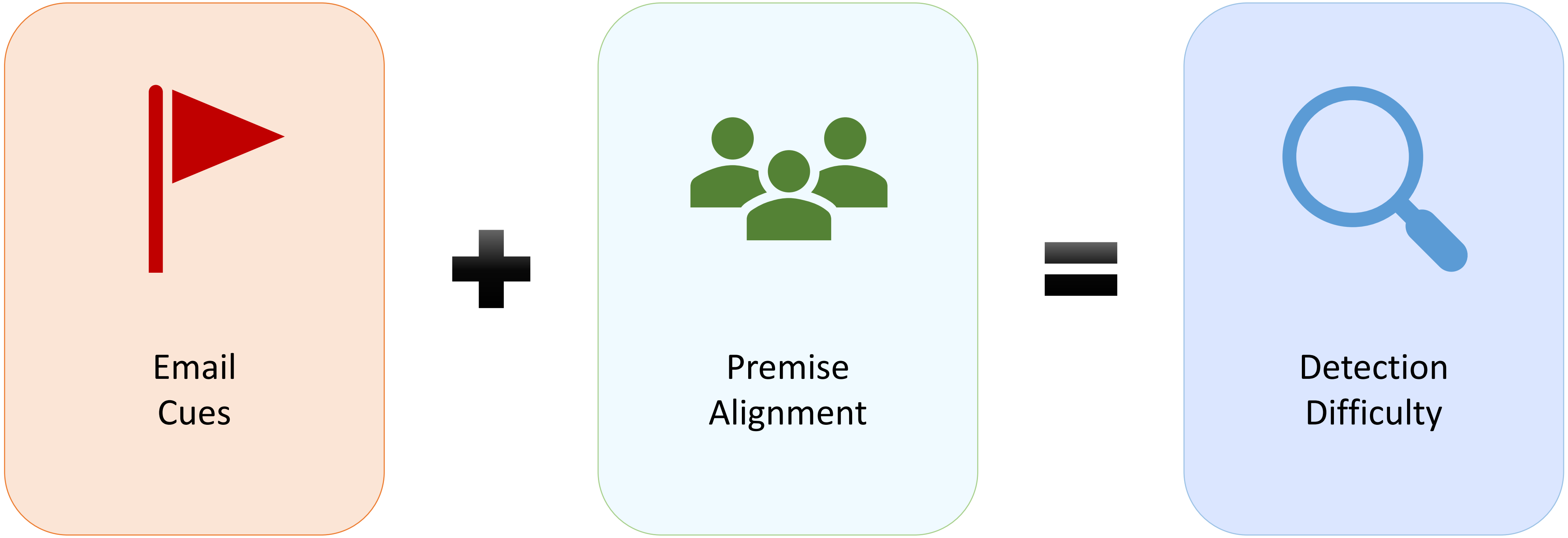
Image credit: NIST

https://www.nist.gov/video/introducing-phish-scale

The NIST Phish Scale

- Created in 2019 using real-world empirical data
- A metric that incorporates the human element to contextualize click rates
- Two components
  - Email cues
  - Premise alignment
- NIST Phish Scale output: detection difficulty rating

NIST Phish Scale Components



Email Cues

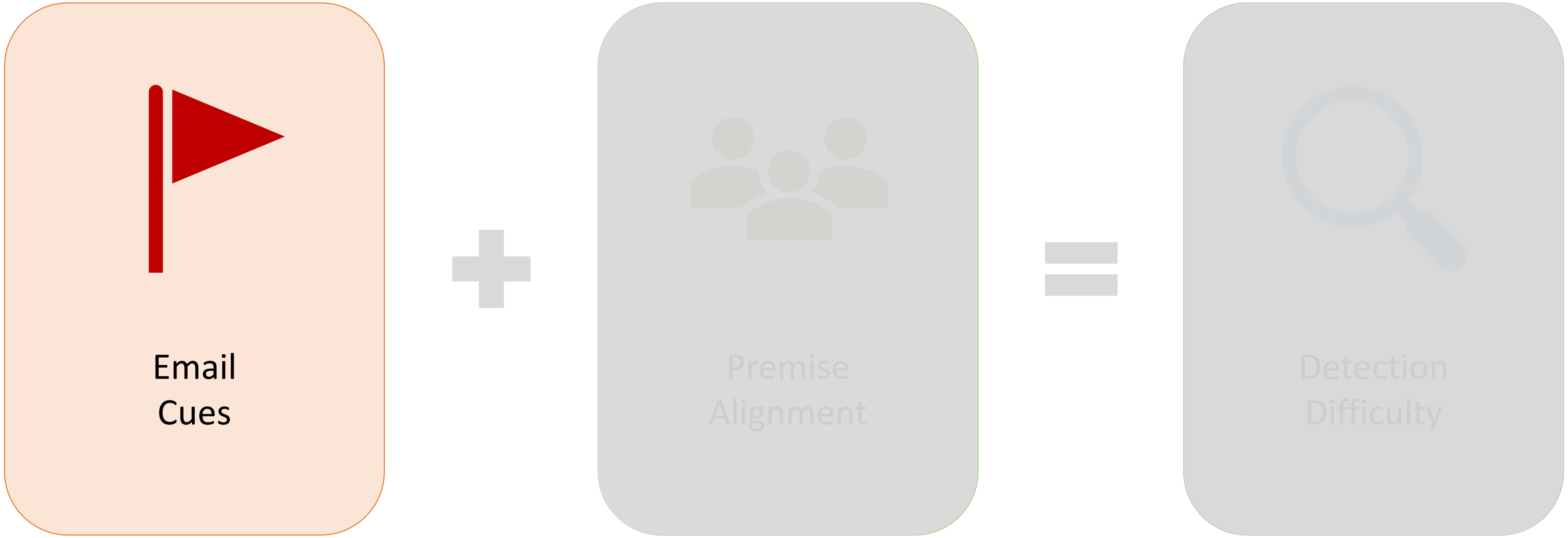
+

Premise Alignment

=

Detection Difficulty

NIST Phish Scale Components



Email Cues

+

Premise Alignment

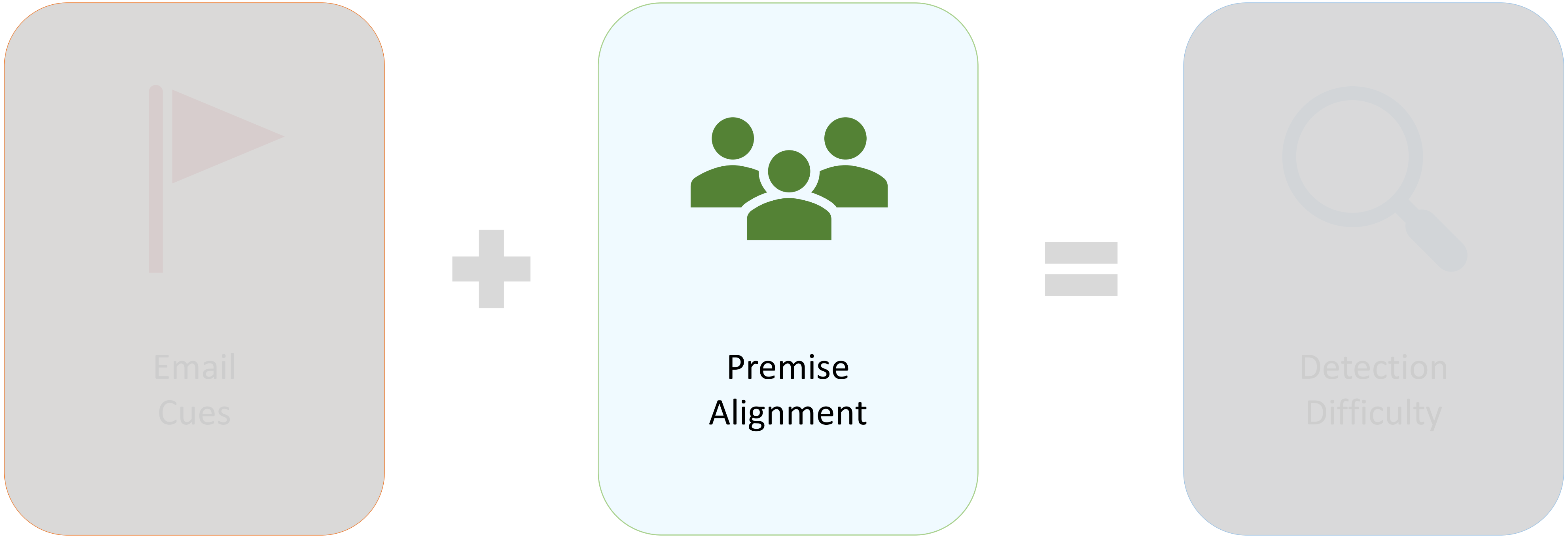
=

Detection Difficulty

NIST Phish Scale – Cues

Images credit: Shutterstock *"McDowell's" credit: https://retruster.com/blog/phishing-email-scams-with-real-phishing-examples.html*

NIST Phish Scale Components



Email Cues + Premise Alignment = Detection Difficulty

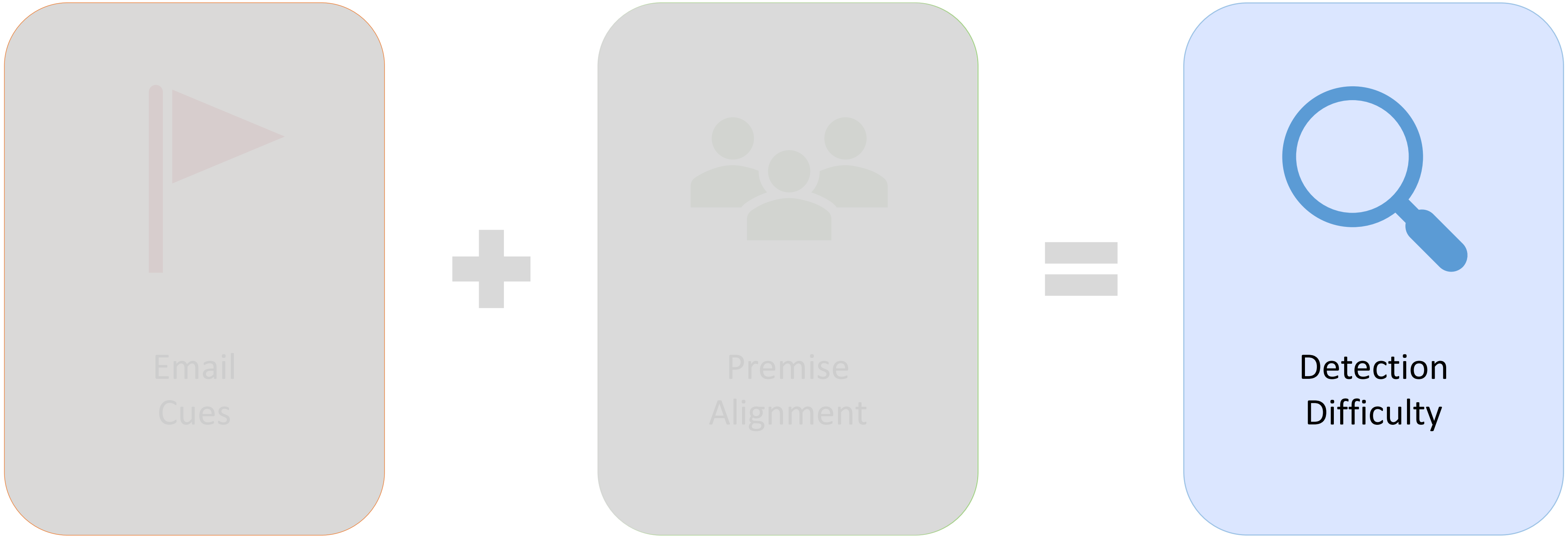
NIST Phish Scale – Premise Alignment

- Characterize relevancy of the email premise for the target audience
  - Based on workplace responsibilities and culture, business practice plausibility, staff expectations
  - Knowledge of target population context of work is crucial for accurate categorization

NIST Phish Scale – Premise Alignment

1. Mimics a workplace process or practice
2. Has workplace relevance
3. Aligns with other situations or events, including external to the workplace
4. Engenders concern over consequences for NOT clicking
5. Has been the subject of targeted training, specific warnings, or other exposure

NIST Phish Scale Components



The NIST Phish Scale – Detection Difficulty

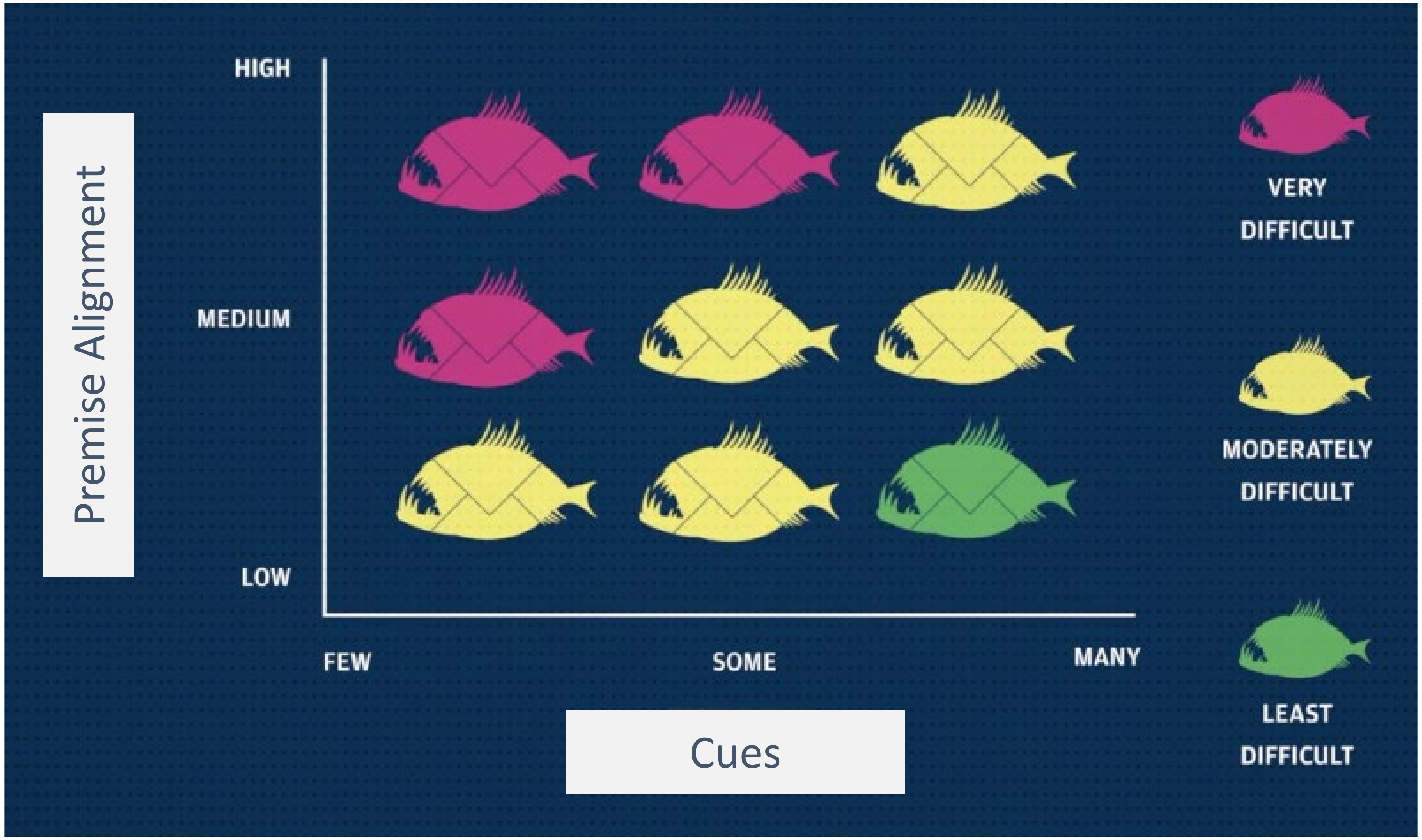
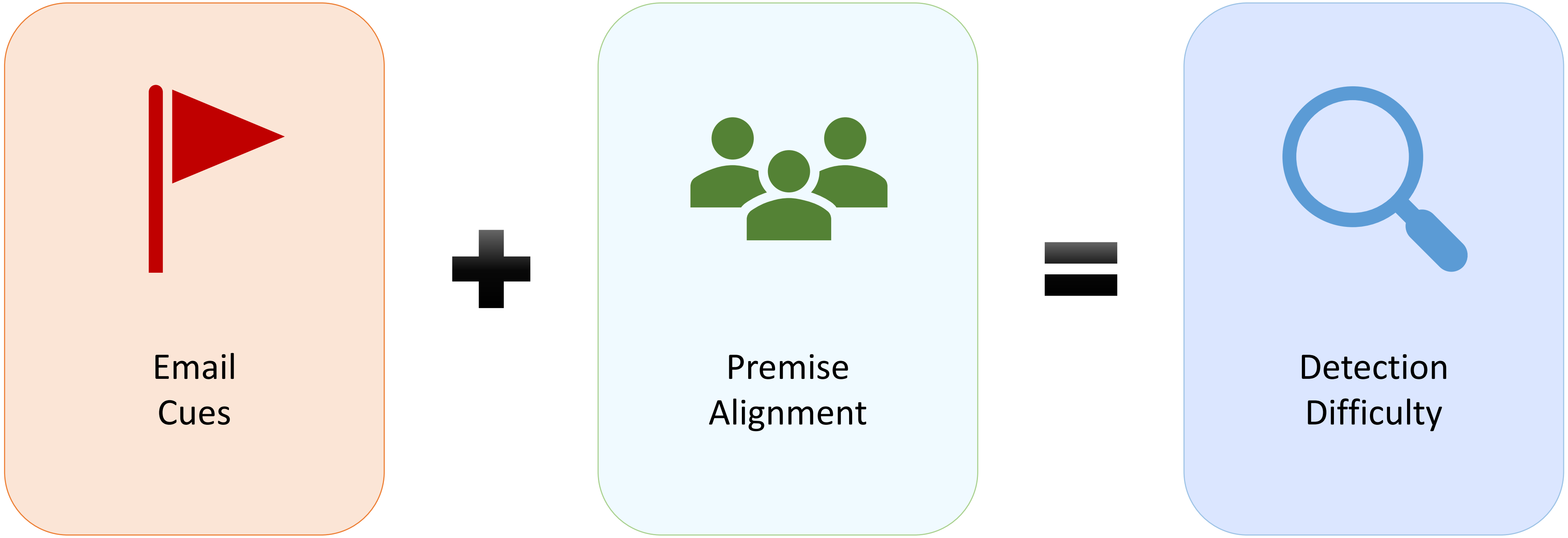


Image credit: NIST

NIST Phish Scale Components



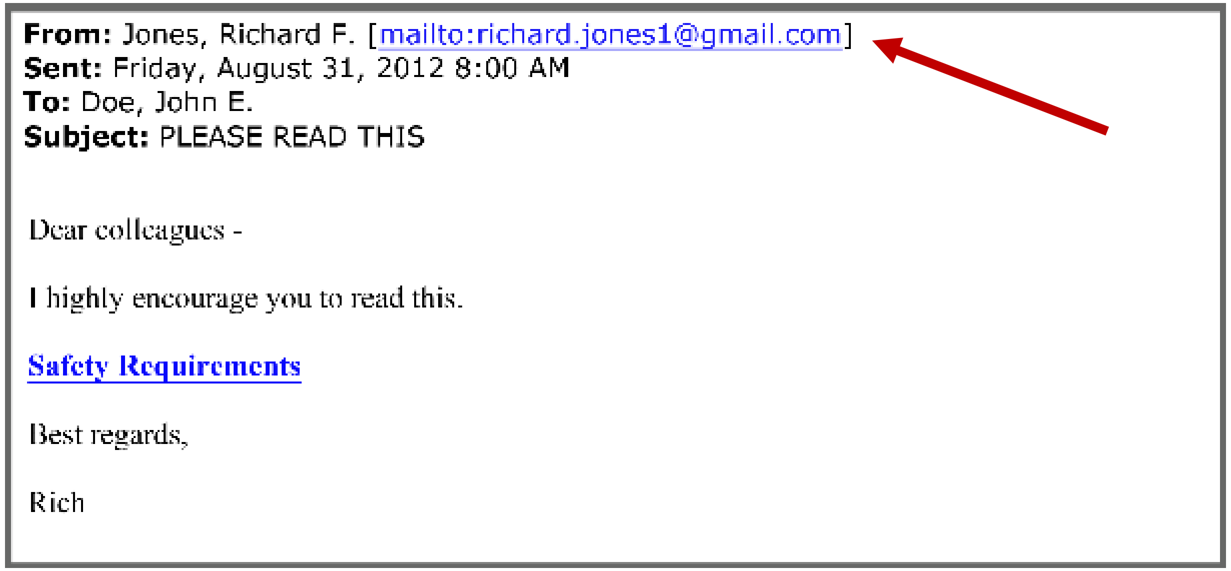
Email Cues

Premise Alignment

Detection Difficulty

Applying the NIST Phish Scale

Applying the NIST Phish Scale



From: Jones, Richard F. [mailto:richard.jones1@gmail.com]
Sent: Friday, August 31, 2012 8:00 AM
To: Doe, John E.
Subject: PLEASE READ THIS

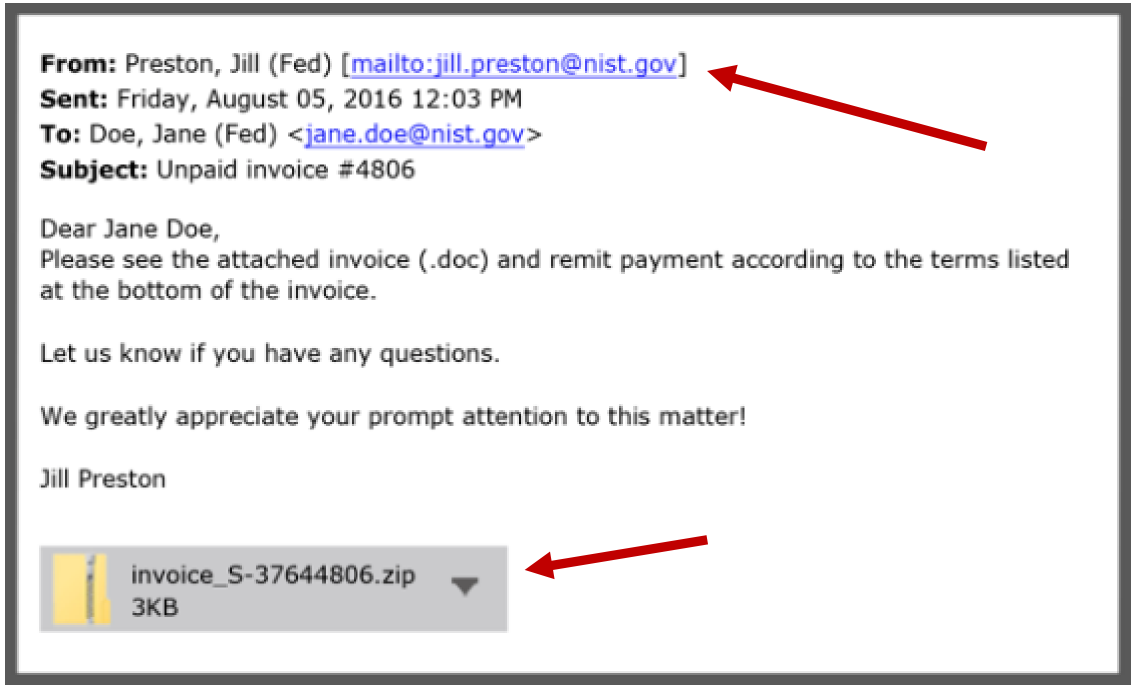
Dear colleagues -

I highly encourage you to read this.

Safety Requirements

Best regards,

Rich



From: Preston, Jill (Fed) [mailto:jill.preston@nist.gov]
Sent: Friday, August 05, 2016 12:03 PM
To: Doe, Jane (Fed) <jane.doe@nist.gov>
Subject: Unpaid invoice #4806

Dear Jane Doe,
Please see the attached invoice (.doc) and remit payment according to the terms listed at the bottom of the invoice.

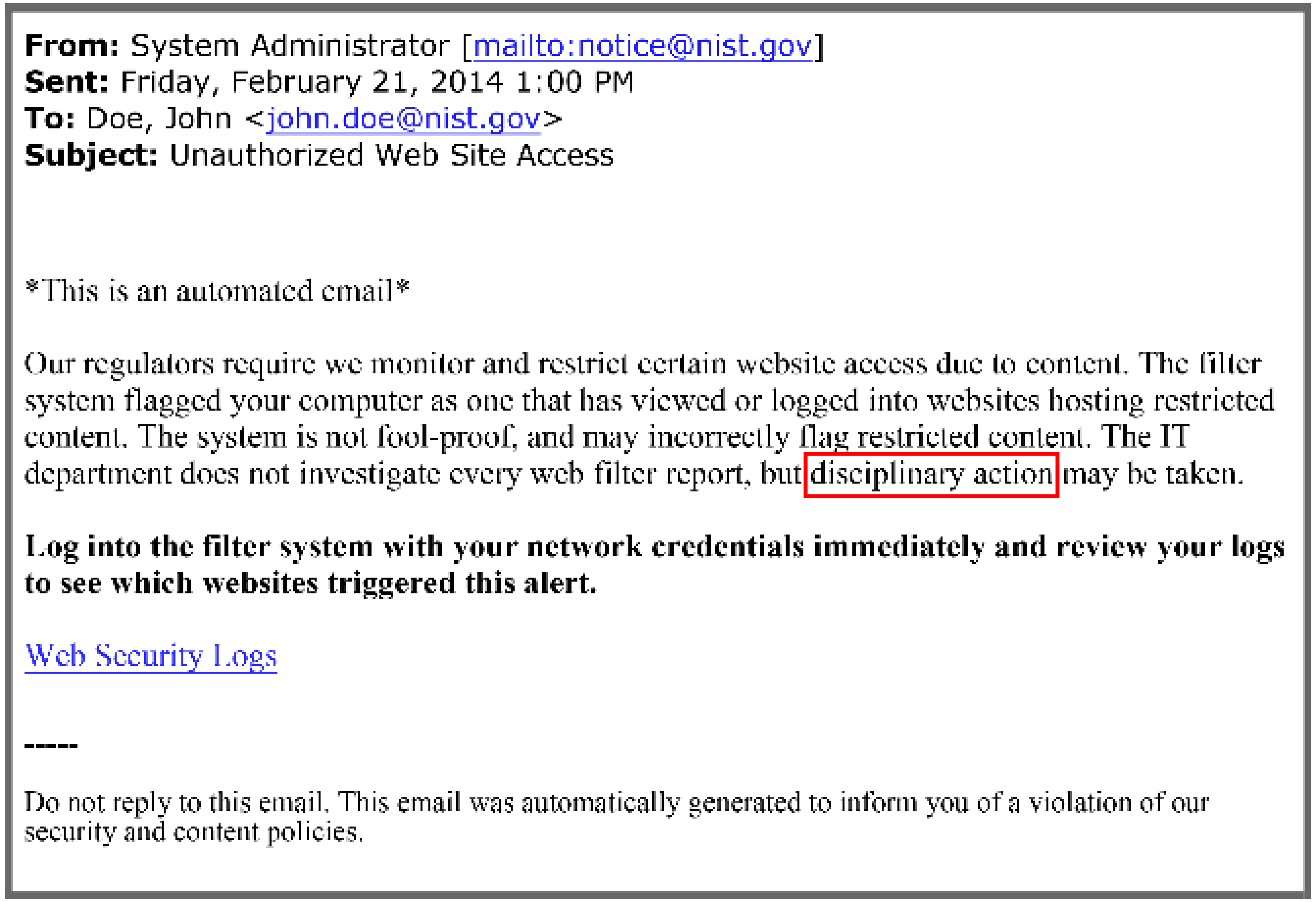
Let us know if you have any questions.

We greatly appreciate your prompt attention to this matter!

Jill Preston

invoice_S-37644806.zip
3KB

Applying the NIST Phish Scale



From: System Administrator [mailto:notice@nist.gov]
Sent: Friday, February 21, 2014 1:00 PM
To: Doe, John <john.doe@nist.gov>
Subject: Unauthorized Web Site Access

This is an automated email

Our regulators require we monitor and restrict certain website access due to content. The filter system flagged your computer as one that has viewed or logged into websites hosting restricted content. The system is not fool-proof, and may incorrectly flag restricted content. The IT department does not investigate every web filter report, but disciplinary action may be taken.

Log into the filter system with your network credentials immediately and review your logs to see which websites triggered this alert.

Web Security Logs

Do not reply to this email. This email was automatically generated to inform you of a violation of our security and content policies.

Applying the NIST Phish Scale Broadly

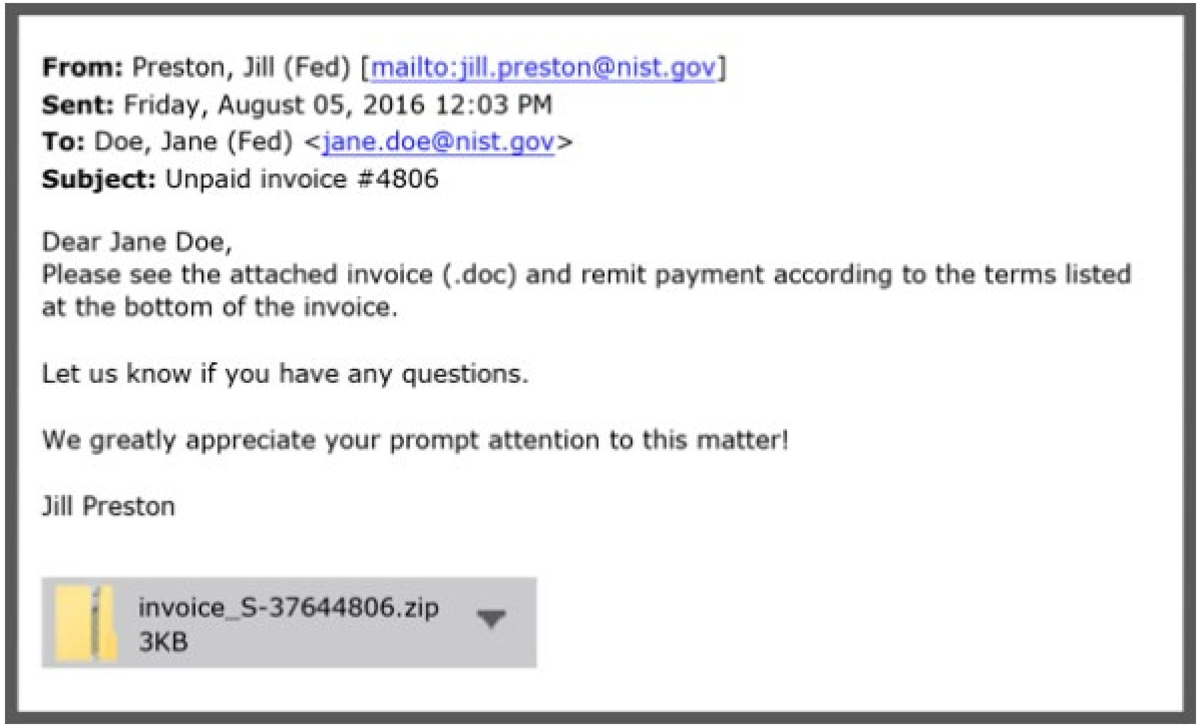
- Designed to use a target audience
- Many organizations conduct phishing training and exercises as a one-size-fits-all approach
- Question: How to apply NIST Phish Scale to whole organization accurately?

Image credit: Shutterstock

Applying the NIST Phish Scale – Workplace Relevance

- How pertinent is the email to the work of the target audience?
- Different detection difficulty ratings for different job families:
  - Administrative support
  - Core mission employees
  - Facilities – field
  - Facilities – office
  - Legal
  - Management
  - Organization support staff

Applying the NIST Phish Scale – Workplace Relevance



From: Preston, Jill (Fed) [mailto:jill.preston@nist.gov]
Sent: Friday, August 05, 2016 12:03 PM
To: Doe, Jane (Fed) <jane.doe@nist.gov>
Subject: Unpaid invoice #4806

Dear Jane Doe,
Please see the attached invoice (.doc) and remit payment according to the terms listed at the bottom of the invoice.

Let us know if you have any questions.

We greatly appreciate your prompt attention to this matter!

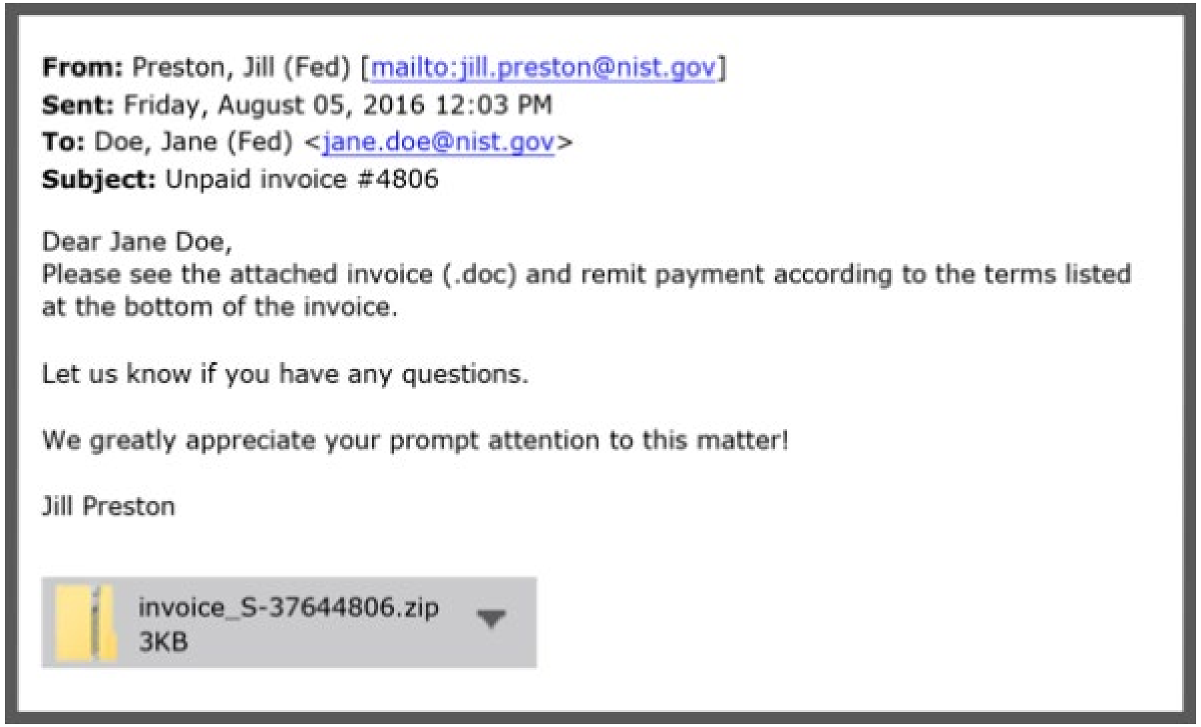
Jill Preston

invoice_S-37644806.zip
3KB

Whole Organization Application

Workplace Relevance: Low
Premise Alignment: Low
Detection Difficulty: Least to Moderate

Applying the NIST Phish Scale – Workplace Relevance



From: Preston, Jill (Fed) [mailto:jill.preston@nist.gov]
Sent: Friday, August 05, 2016 12:03 PM
To: Doe, Jane (Fed) <jane.doe@nist.gov>
Subject: Unpaid invoice #4806

Dear Jane Doe,
Please see the attached invoice (.doc) and remit payment according to the terms listed at the bottom of the invoice.

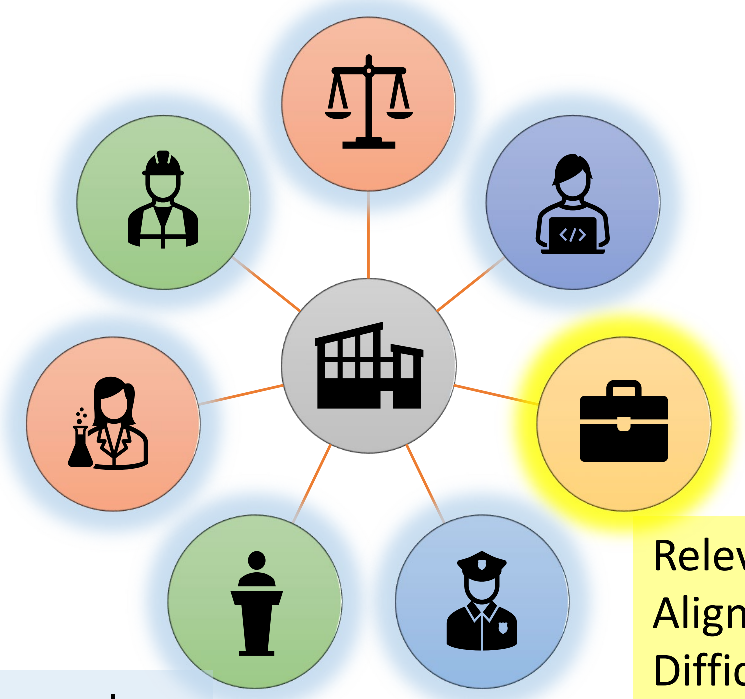
Let us know if you have any questions.

We greatly appreciate your prompt attention to this matter!

Jill Preston

invoice_S-37644806.zip
3KB

Job Family Application



Relevance: High
Alignment: High
Difficulty: Very

Relevance: Low
Alignment: Low
Difficulty: Least

Summary

NIST

Multi-Pronged

Organizational phishing defense

Click rates

Click rates will not go to zero!
(and stay there)

User context

Understand human element to contextualize click rates with the NIST Phish Scale

No silver bullet

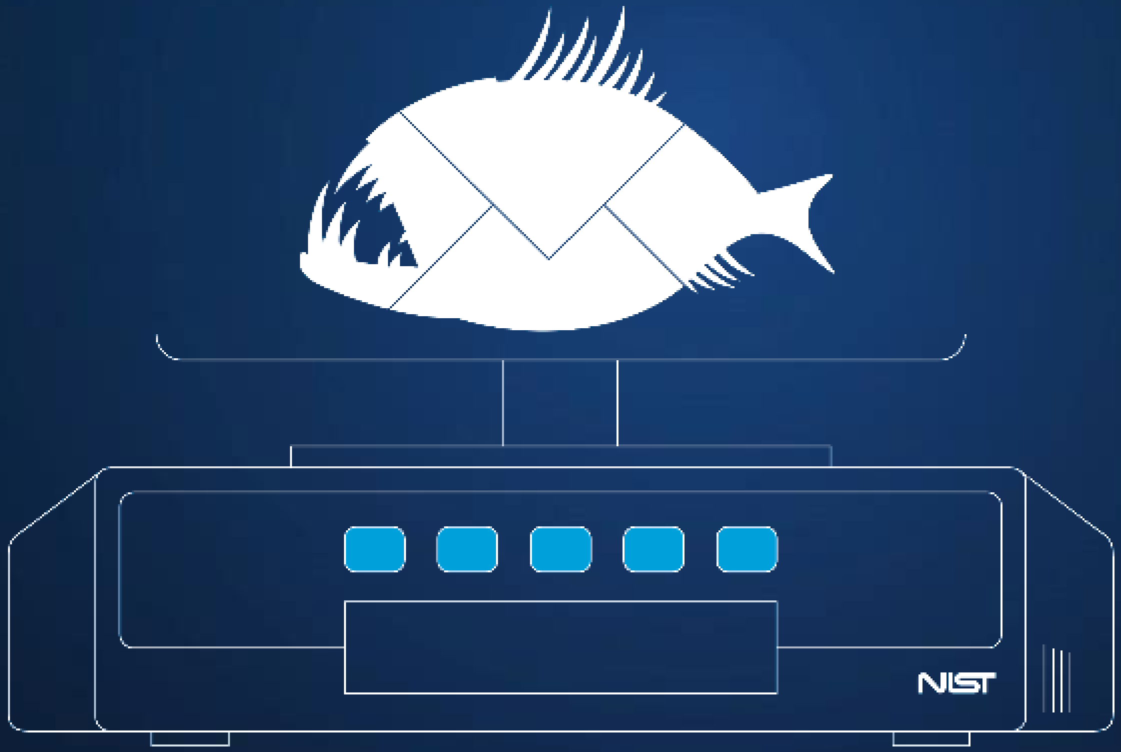
Awareness training is not the silver bullet in phishing defense

Additional Resources

- Shanée Dawkins, dawkins@nist.gov
- Jody Jacobs, jody.jacobs@nist.gov

- https://csrc.nist.gov/projects/usable-cybersecurity
- https://csrc.nist.gov/usable-cybersecurity/phishing

NIST Phishing Research



Q&A

The Future With AI

Tushar Rathod
Enterprise Architecture
Social Security Administration

fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

#FISSEA2023

The future with AI

Tushar Rathod

Artificial Intelligence (AI) is revolutionizing the way we live and work.

It can solve big problems facing us today.

AI Use Cases:

1. Affordable personalized medicine
2. Fraud detection at source
3. Real-time customer sentiment analysis & response
4. Combating climate change

AI in Healthcare

- Zero wait time
- Rapid diagnosis
- Personalized treatment plans
- Automated robotic surgery
- Gene editing
- Treat cancer & other chronic diseases

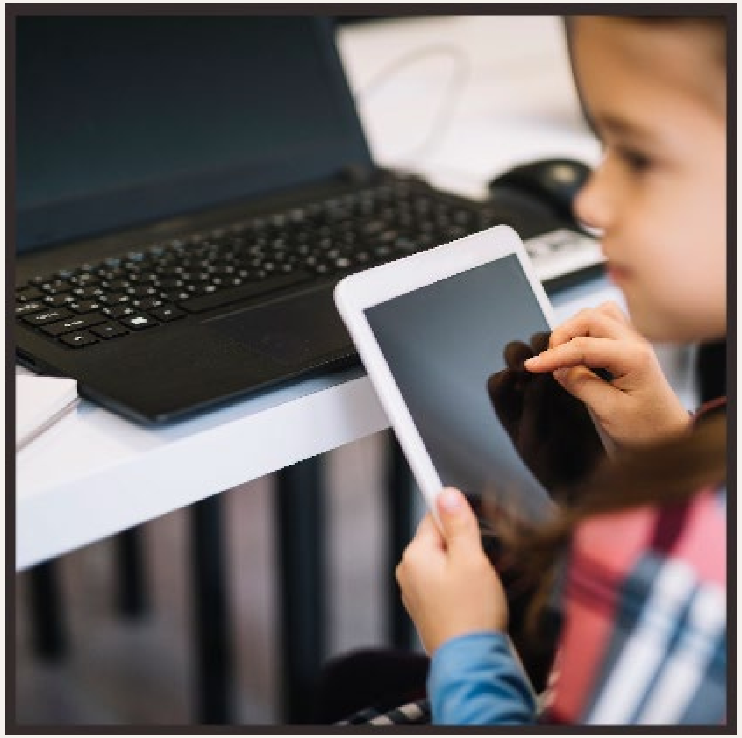
"Death will be optional by 2045!"

AI in Education

- Education & "going to school"
- Personalized learning
- Extremely affordable
- Highly effective and truly enjoyable!

Align -

- what I am good at,
- what I want to do, and
- what I can get paid to do



Should students be allowed to use Chat GPT?

What should the universities teach and why?

What can the future AI NOT do (or not as well as humans)?

AI in Business

From routine task automation to solving highly complex problems:

- Autonomous mining operations
- Deep sea exploration, mining & rescue
- Optimized diamond polishing
- Predict customer behavior & buying patterns
- Accurate economic & business forecasts
- Help manage cultural transformations

Businesses will be created by AI,
will use AI or
will be destroyed by AI.

AI Assistant

What if someone "really knew me, and understood me"? Some potential use cases:

- Give me company! Be my sounding board.
- Fill out my medical forms, take my surveys!
- What should I eat today?
  Yes, make it for me!
- Take me to my next appointment on time
- Plan my summer family vacation
- Find my pet!

Will AI ever replace your best friend?

AI in Government

AI has the power to transform government services in numerous ways:

- Efficient allocation of public funds
- Expedient service delivery
- Enhanced public safety
- Highly effective social services
- Outcome driven policy modeling
- Accessibility
- Eliminate tax evasion

Would you vote for an AI-powered government?

The Future of AI

- It is early days for AI
- The promise is great!
- Thoughtful, future-centric regulation is much needed
- One of the most transformational technologies ever
- Complimented by Quantum computing, the possibilities are endless
- As with any technology, the downside needs to be carefully managed

Today's AI is akin to a calculator that holds the promise of evolving into "cloud computing" in the near future.

Conclusion

AI has the potential to transform every aspect of our lives, from healthcare and education to business, government and beyond.

How will we collectively shape AI?

And how will AI shape us?

Thank you!

This presentation was assisted by AI (ChatGPT 3.5 and Wepik) including slide creation & the graphics.
The future is here!

Questions?

This presentation was assisted by AI (ChatGPT 3.5 and Wepik) including slide creation & the graphics.
The future is here!

Role-Based Training, An Epic Tale of Woe and Triumph

Morgan Floyd

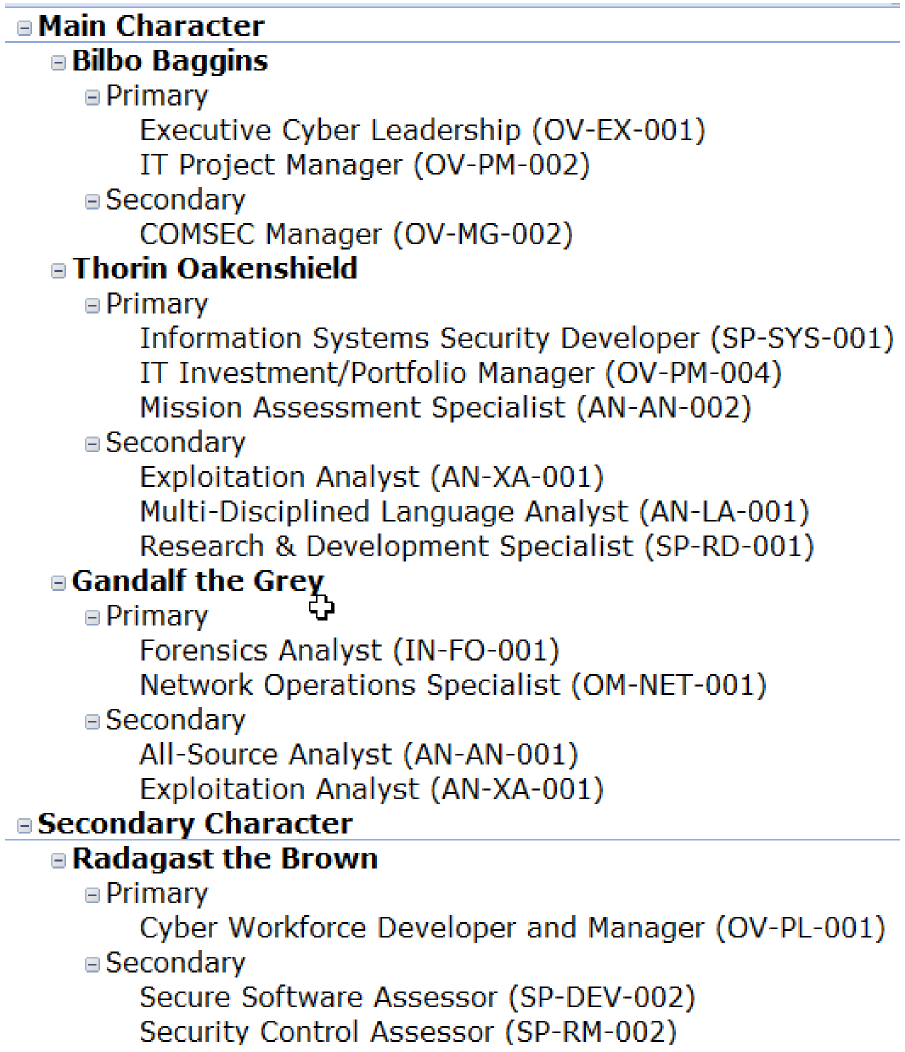
InfoSec Training & Awareness Coordinator
Cyber Assurance
Texas Health & Human Services

Role-based Training

AN EPIC TALE OF WOE AND TRIUMPH

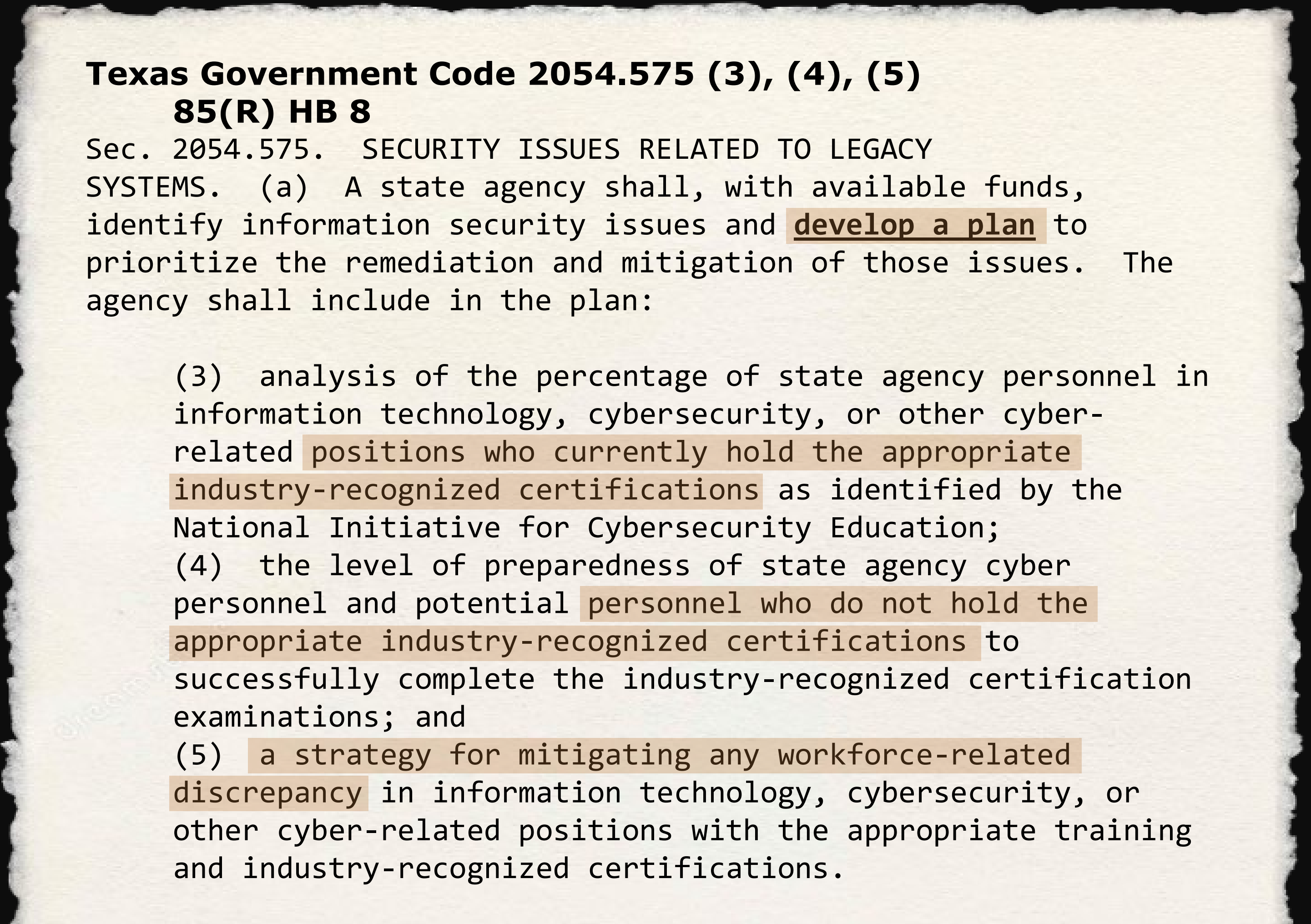
TERMS OF NOTE

NICE Framework Mapping – The assignment of work roles to a person based on the functions and duties they perform for an organization in relation to the tasks of NICE work roles.



- ⊟ **Main Character**
  - ⊟ **Bilbo Baggins**
    - ⊟ Primary
      - Executive Cyber Leadership (OV-EX-001)
      - IT Project Manager (OV-PM-002)
    - ⊟ Secondary
      - COMSEC Manager (OV-MG-002)
  - ⊟ **Thorin Oakenshield**
    - ⊟ Primary
      - Information Systems Security Developer (SP-SYS-001)
      - IT Investment/Portfolio Manager (OV-PM-004)
      - Mission Assessment Specialist (AN-AN-002)
    - ⊟ Secondary
      - Exploitation Analyst (AN-XA-001)
      - Multi-Disciplined Language Analyst (AN-LA-001)
      - Research & Development Specialist (SP-RD-001)
  - ⊟ **Gandalf the Grey**
    - ⊟ Primary
      - Forensics Analyst (IN-FO-001)
      - Network Operations Specialist (OM-NET-001)
    - ⊟ Secondary
      - All-Source Analyst (AN-AN-001)
      - Exploitation Analyst (AN-XA-001)
- ⊟ **Secondary Character**
  - ⊟ **Radagast the Brown**
    - ⊟ Primary
      - Cyber Workforce Developer and Manager (OV-PL-001)
    - ⊟ Secondary
      - Secure Software Assessor (SP-DEV-002)
      - Security Control Assessor (SP-RM-002)

Where it started



Texas Government Code 2054.575 (3), (4), (5)

85(R) HB 8

Sec. 2054.575. SECURITY ISSUES RELATED TO LEGACY SYSTEMS. (a) A state agency shall, with available funds, identify information security issues and **develop a plan** to prioritize the remediation and mitigation of those issues. The agency shall include in the plan:

(3) analysis of the percentage of state agency personnel in information technology, cybersecurity, or other cyber-related positions who currently hold the appropriate industry-recognized certifications as identified by the National Initiative for Cybersecurity Education;

(4) the level of preparedness of state agency cyber personnel and potential personnel who do not hold the appropriate industry-recognized certifications to successfully complete the industry-recognized certification examinations; and

(5) a strategy for mitigating any workforce-related discrepancy in information technology, cybersecurity, or other cyber-related positions with the appropriate training and industry-recognized certifications.

THE GOAL

Develop Information Security Role-Based Training Initiative (IS-RBTI)

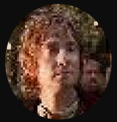
- Identify employees who hold industry recognized certifications
- Identify and close knowledge gaps

THE PLAN

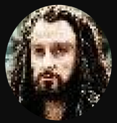
INFORMATION SECURITY ROLE-BASED TRAINING INITIATIVE (IS-RBTI)

Employees

Gandalf



Bilbo Baggins



Thorin Oakenshield

Certifications & Trainings

Wizard
General Meddling

Hobbit
Riddle Master

Dwarf
King Under the Mountain

Work Roles

Work Role 1

Work Role 2

Work Role 3

Work Role 4

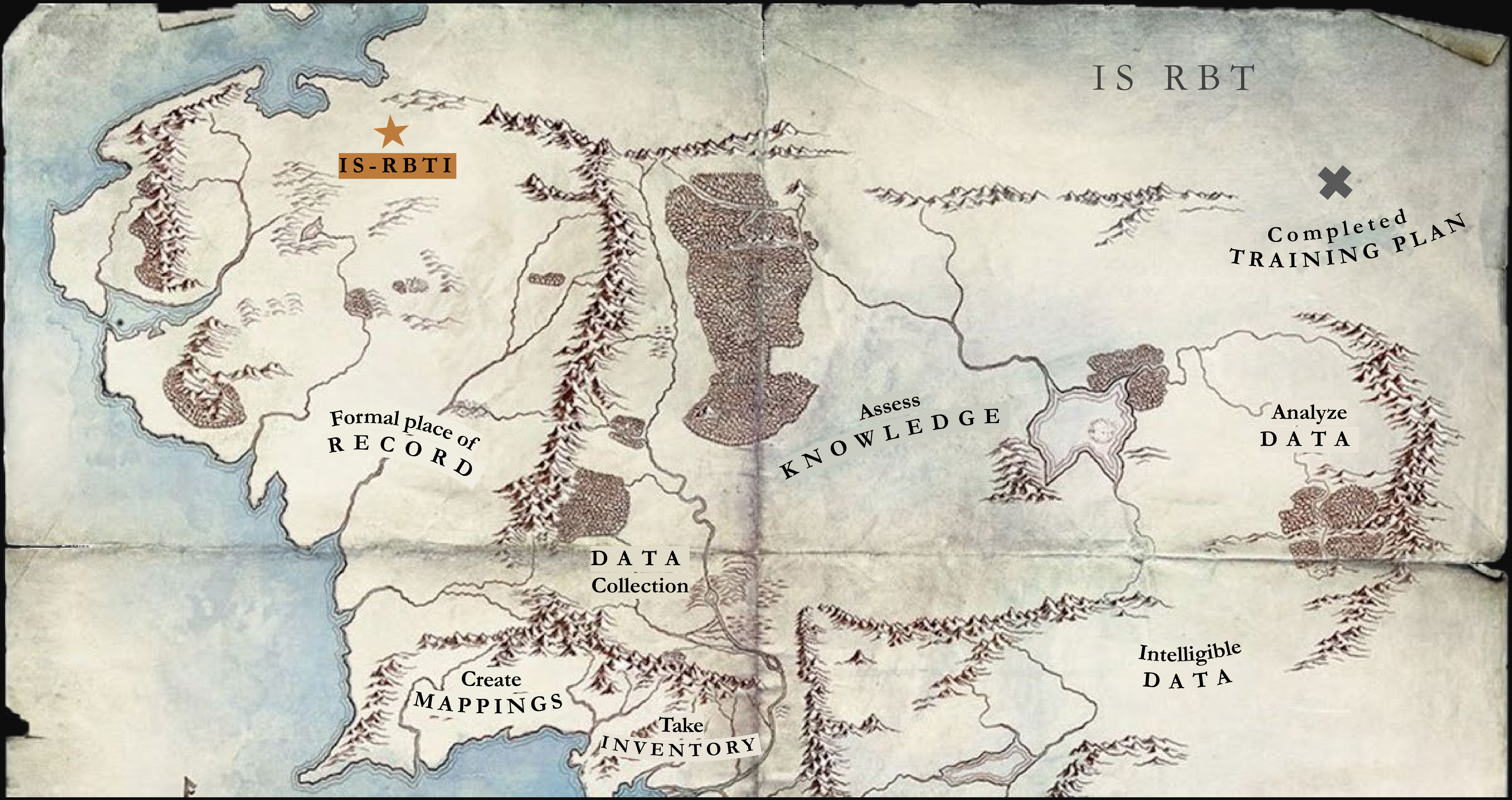
Work Role 5

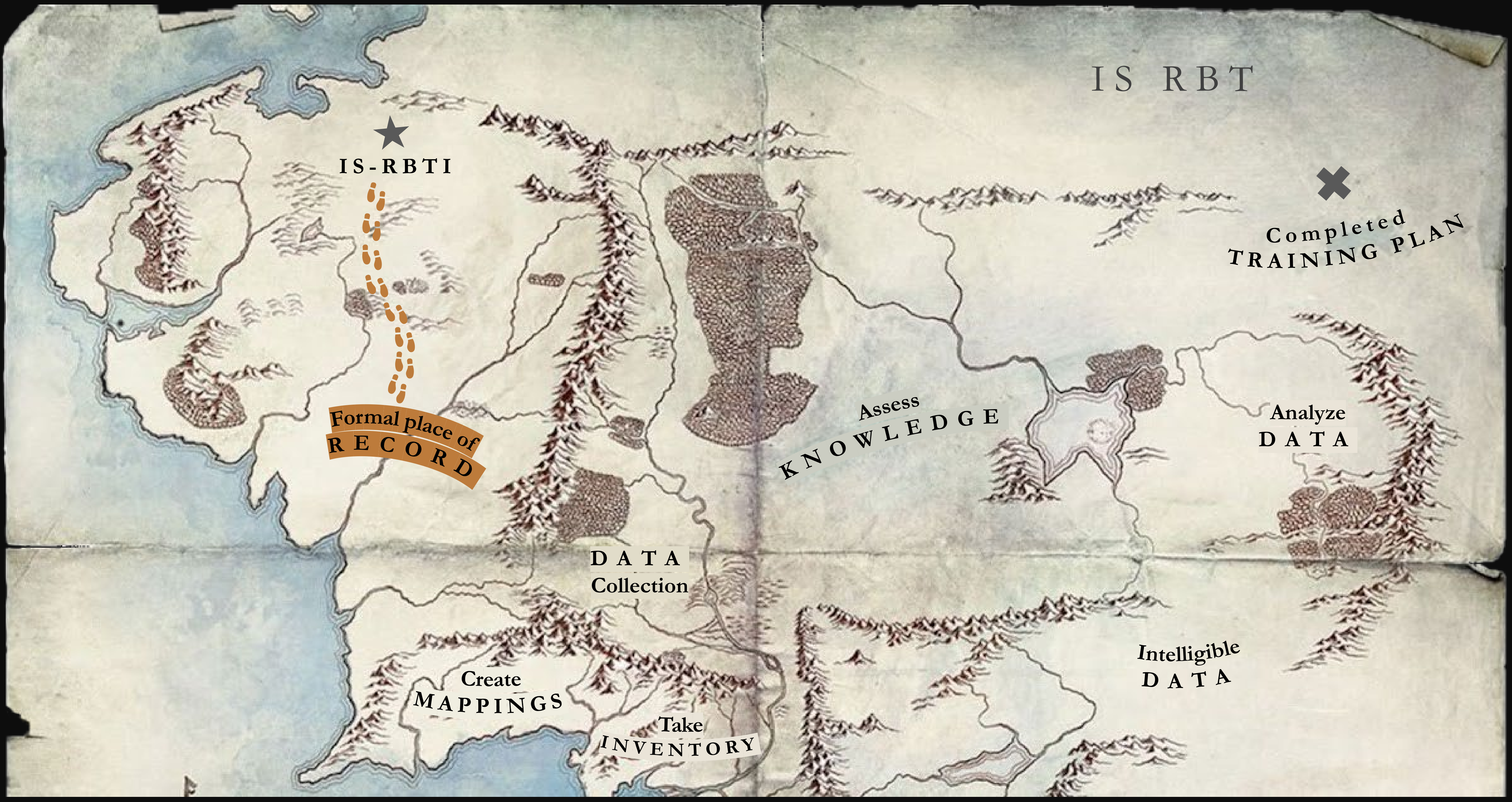
Work Role 6

Select effective training for each employee

THE JOURNEY BEGINS

YEAR ONE


IS RBT
★ IS-RBTI
✖ Completed TRAINING PLAN
Formal place of RECORD
Assess KNOWLEDGE
Analyze DATA
DATA Collection
Create MAPPINGS
Take INVENTORY
Intelligible DATA



IS RBT

IS-RBTI

Formal place of RECORD

DATA Collection

Create MAPPINGS

Take INVENTORY

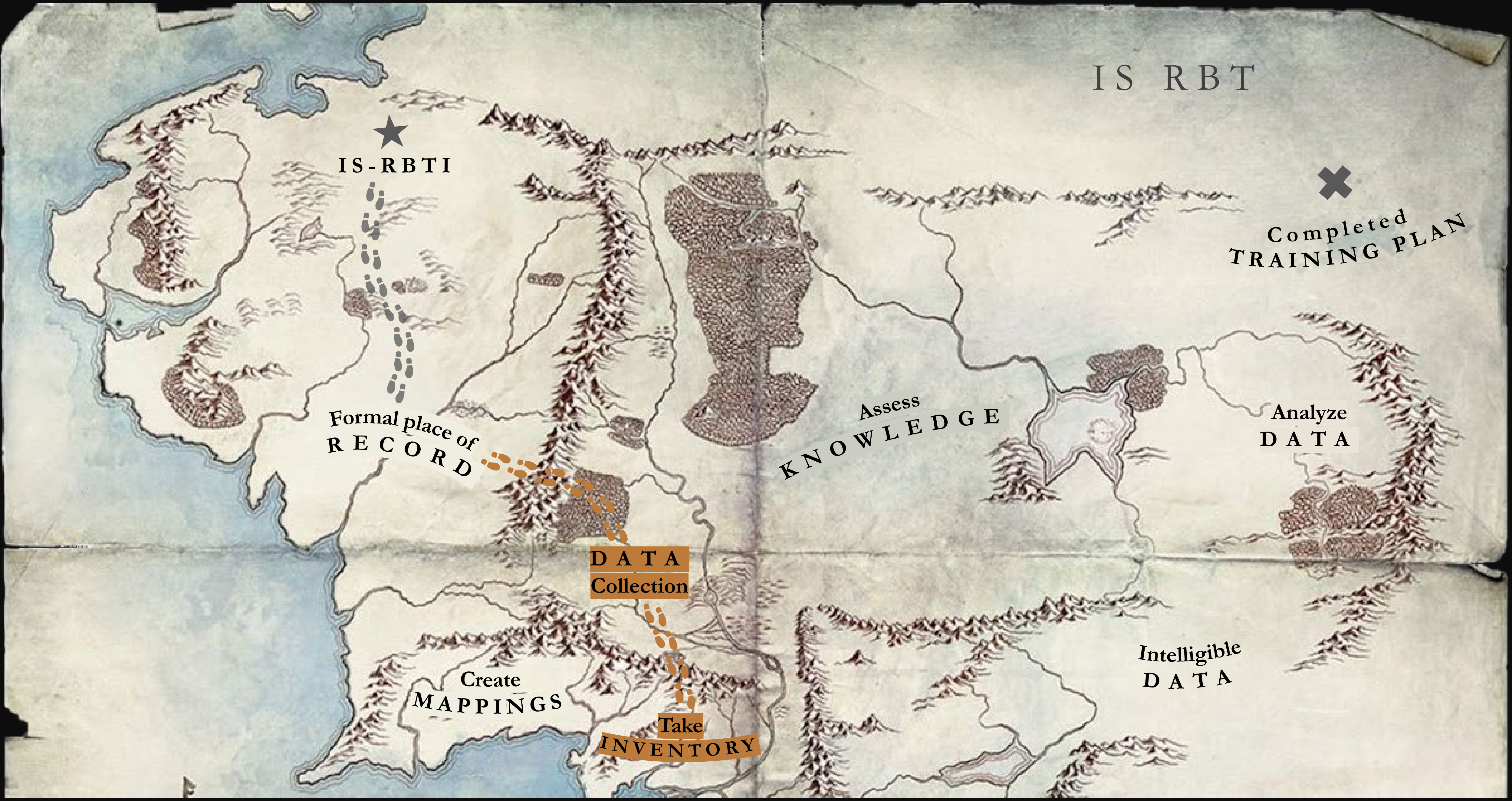
Assess KNOWLEDGE

Analyze DATA

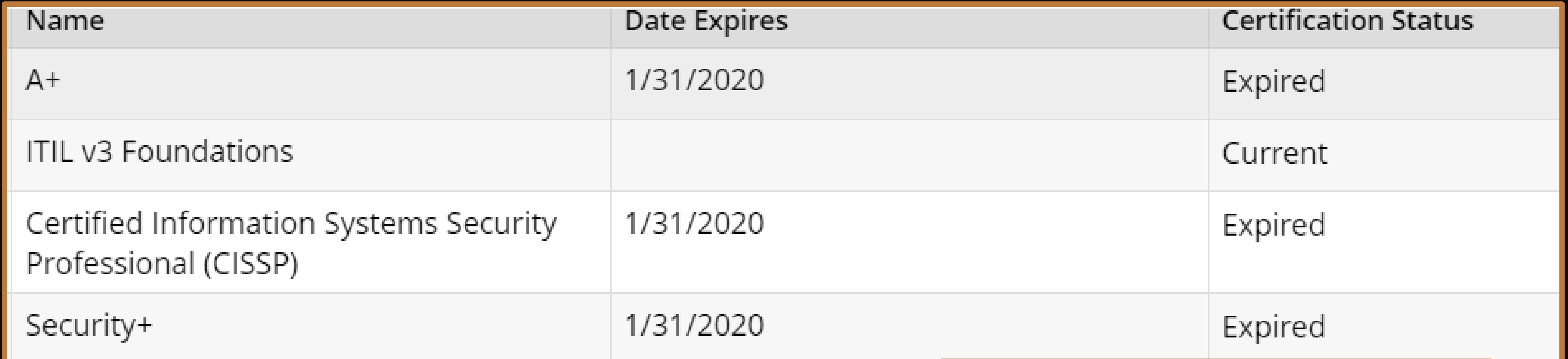
Intelligible DATA

Completed TRAINING PLAN

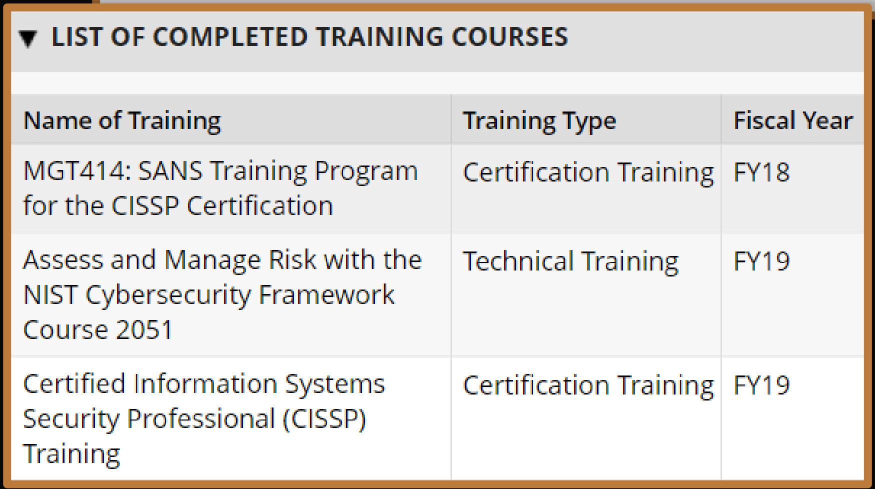
IS RBT


IS-RBTI
Formal place of RECORD
DATA Collection
Take INVENTORY
Create MAPPINGS
Assess KNOWLEDGE
Analyze DATA
Intelligible DATA
Completed TRAINING PLAN

Take inventory

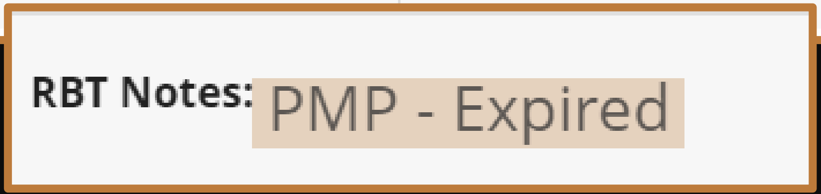


Name	Date Expires	Certification Status
A+	1/31/2020	Expired
ITIL v3 Foundations		Current
Certified Information Systems Security Professional (CISSP)	1/31/2020	Expired
Security+	1/31/2020	Expired



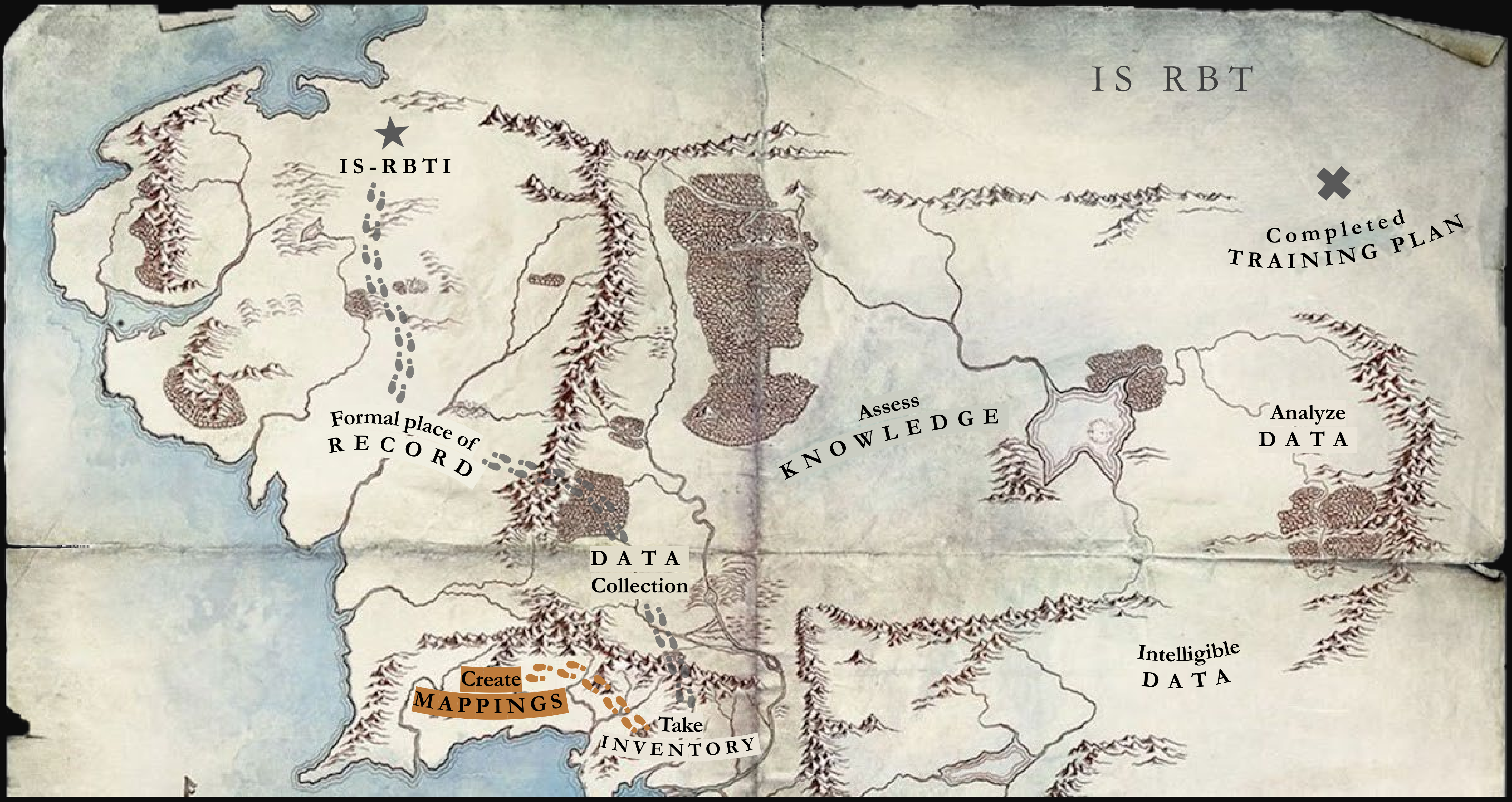
▼ LIST OF COMPLETED TRAINING COURSES

Name of Training	Training Type	Fiscal Year
MGT414: SANS Training Program for the CISSP Certification	Certification Training	FY18
Assess and Manage Risk with the NIST Cybersecurity Framework Course 2051	Technical Training	FY19
Certified Information Systems Security Professional (CISSP) Training	Certification Training	FY19



RBT Notes: PMP - Expired

IS RBT



IS-RBTI

Formal place of RECORD

DATA Collection

Take INVENTORY

Create MAPPINGS

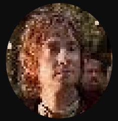
Intelligible DATA

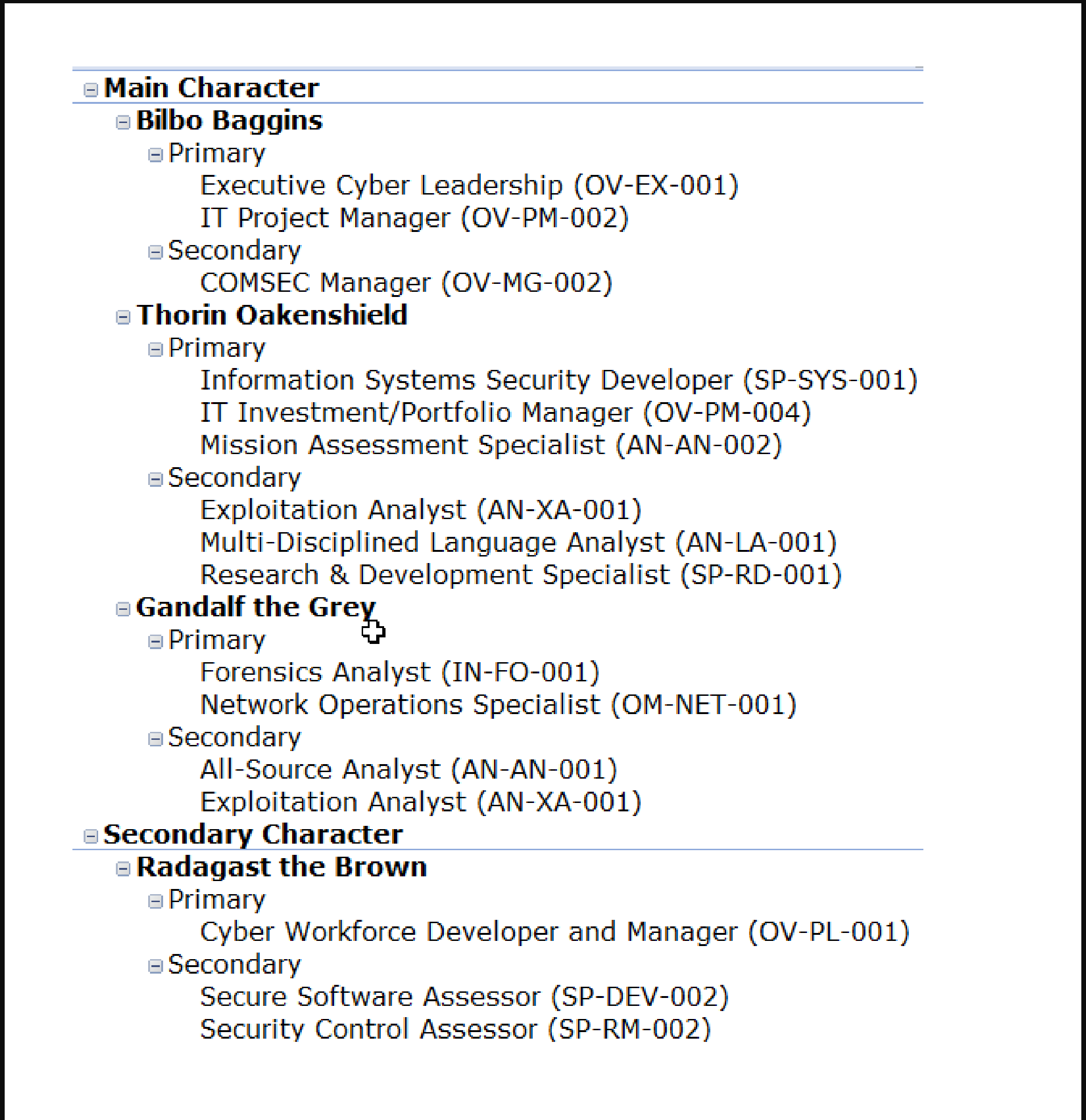
Analyze DATA

Assess KNOWLEDGE

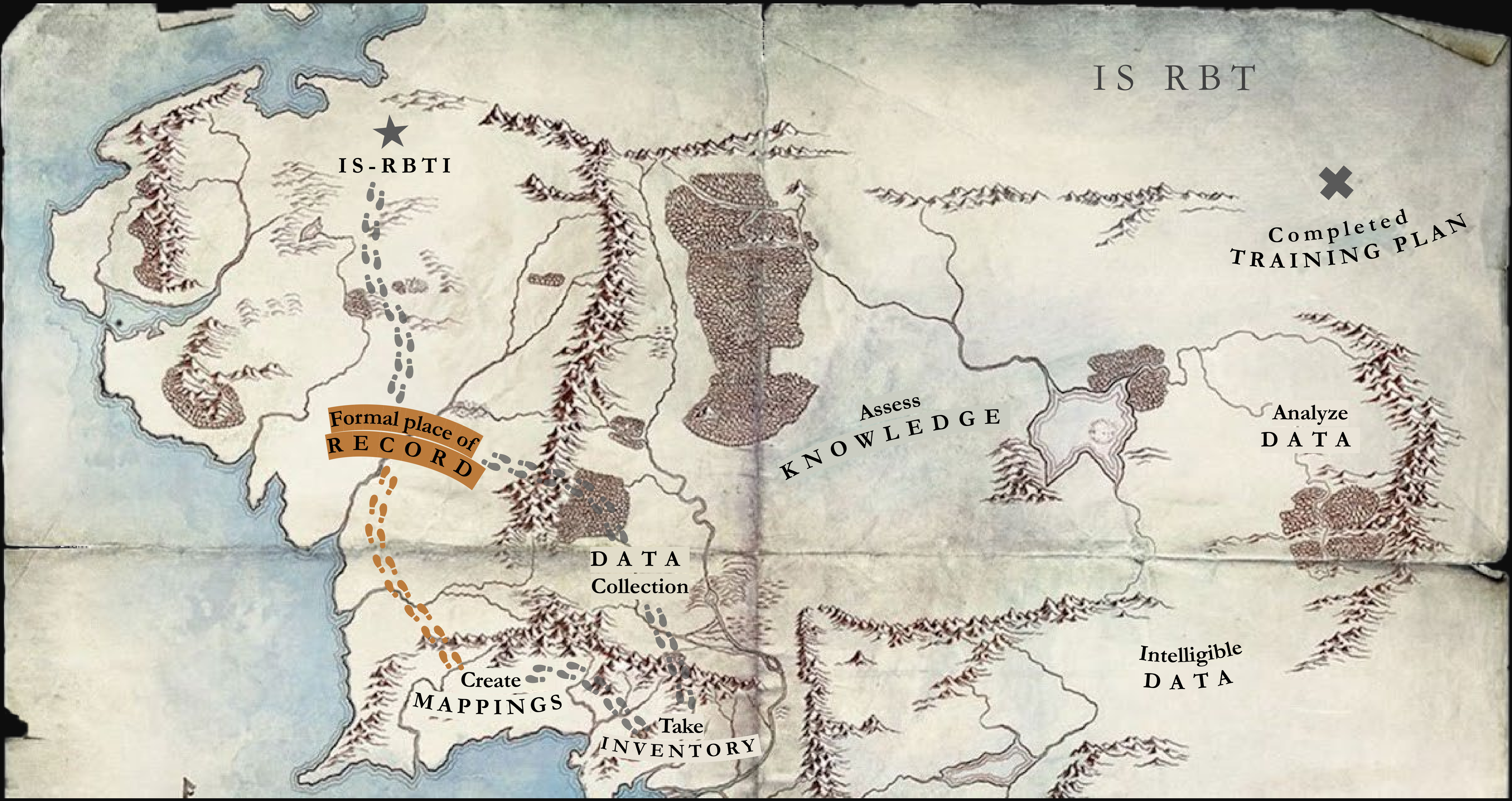
Completed TRAINING PLAN

Create NICE Mapping

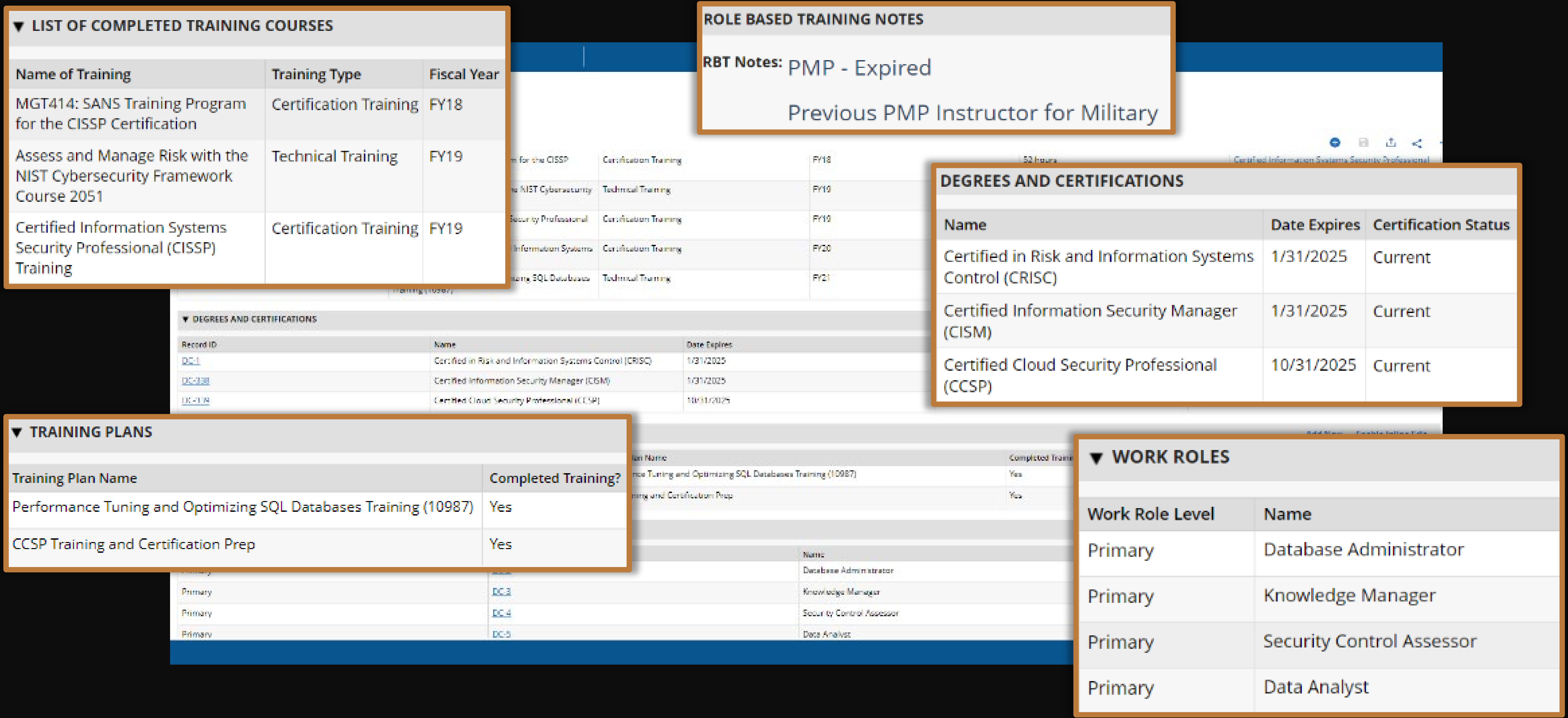
Staff Member	Function	NICE Roles Based on Daily Job Functions and Responsibilities
Gandalf	Primary	Vulnerability Assessment Analyst – (PR-VAM-001)
		Threat/Warning Analyst – (AN-TWA-001)
		Exploitation Analyst – (AN-EXP-001)
	Secondary	Cyber Defense Forensic Analyst – (IN-FOR-002)
		All Source Analyst – (AN-ASA-001)
		System Administrator – (OM-ADM-001)
		System Security Analyst – (OM-ANA-001)
		Cyber Defense Analyst – (PR-CDA-001)
		Cyber Defense Infrastructure Support Specialist – (PR-INF-001)
		Cyber Defense Incident Responder – (PR-CIR-001)
 Bilbo Baggins	Primary	Cyber Defense Forensic Analyst (IN-FOR-002)
		Cyber Defense Incident Responder – (PR-CDA-001)
		All Source Analyst – (AN-ASA-001)
	Secondary	Cyber Policy and Strategy Planner (OV-SPP-002)



- ⊟ **Main Character**
  - ⊟ **Bilbo Baggins**
    - ⊟ Primary
      - Executive Cyber Leadership (OV-EX-001)
      - IT Project Manager (OV-PM-002)
    - ⊟ Secondary
      - COMSEC Manager (OV-MG-002)
  - ⊟ **Thorin Oakenshield**
    - ⊟ Primary
      - Information Systems Security Developer (SP-SYS-001)
      - IT Investment/Portfolio Manager (OV-PM-004)
      - Mission Assessment Specialist (AN-AN-002)
    - ⊟ Secondary
      - Exploitation Analyst (AN-XA-001)
      - Multi-Disciplined Language Analyst (AN-LA-001)
      - Research & Development Specialist (SP-RD-001)
  - ⊟ **Gandalf the Grey**
    - ⊟ Primary
      - Forensics Analyst (IN-FO-001)
      - Network Operations Specialist (OM-NET-001)
    - ⊟ Secondary
      - All-Source Analyst (AN-AN-001)
      - Exploitation Analyst (AN-XA-001)
- ⊟ **Secondary Character**
  - ⊟ **Radagast the Brown**
    - ⊟ Primary
      - Cyber Workforce Developer and Manager (OV-PL-001)
    - ⊟ Secondary
      - Secure Software Assessor (SP-DEV-002)
      - Security Control Assessor (SP-RM-002)


IS RBT
IS-RBTI
Formal place of RECORD
DATA Collection
Create MAPPINGS
Take INVENTORY
Assess KNOWLEDGE
Analyze DATA
Intelligible DATA
Completed TRAINING PLAN

Formal place of record



▼ LIST OF COMPLETED TRAINING COURSES

Name of Training	Training Type	Fiscal Year
MGT414: SANS Training Program for the CISSP Certification	Certification Training	FY18
Assess and Manage Risk with the NIST Cybersecurity Framework Course 2051	Technical Training	FY19
Certified Information Systems Security Professional (CISSP) Training	Certification Training	FY19

ROLE BASED TRAINING NOTES

RBT Notes: PMP - Expired

Previous PMP Instructor for Military

DEGREES AND CERTIFICATIONS

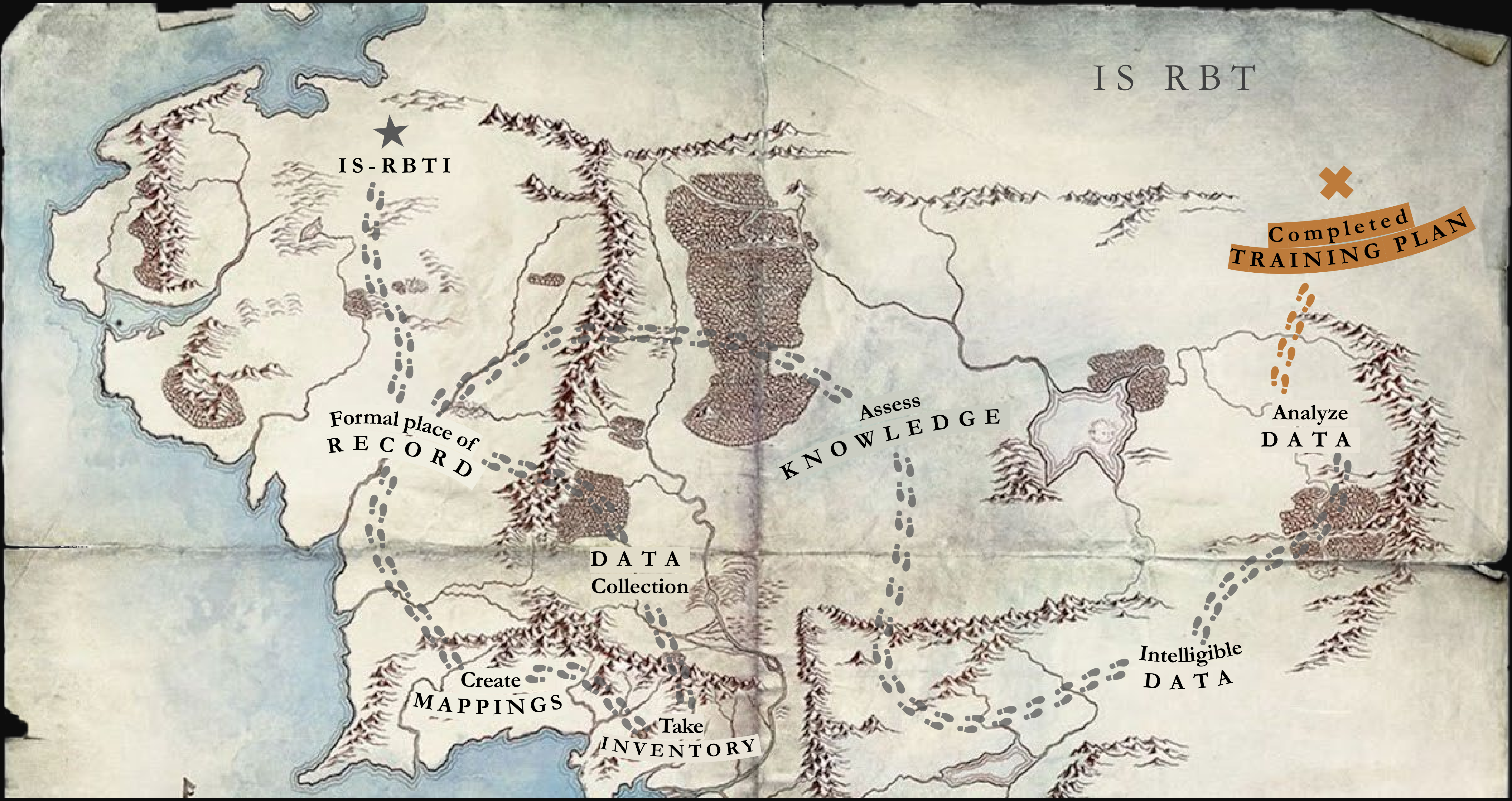
Name	Date Expires	Certification Status
Certified in Risk and Information Systems Control (CRISC)	1/31/2025	Current
Certified Information Security Manager (CISM)	1/31/2025	Current
Certified Cloud Security Professional (CCSP)	10/31/2025	Current

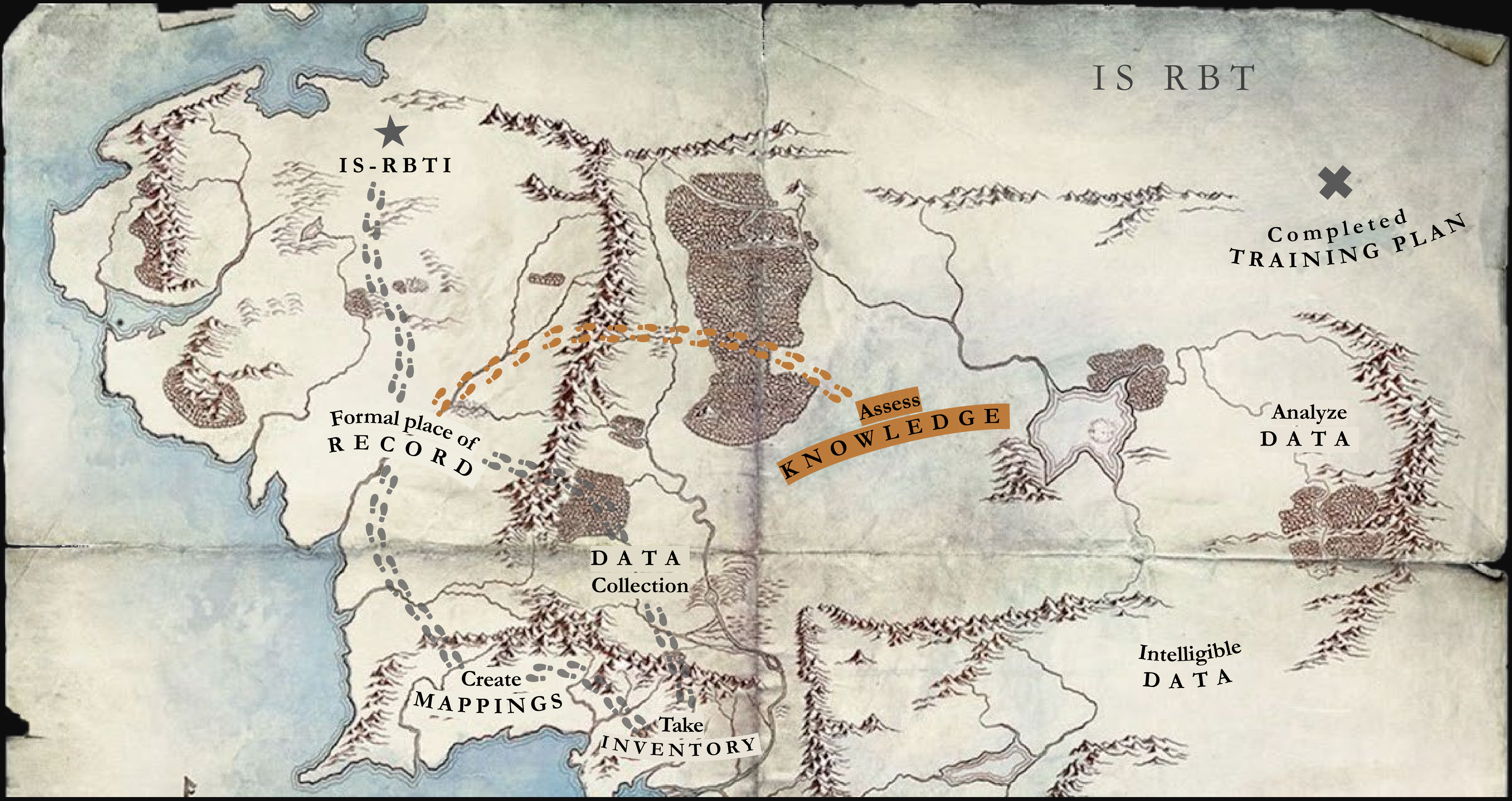
▼ TRAINING PLANS

Training Plan Name	Completed Training?
Performance Tuning and Optimizing SQL Databases Training (10987)	Yes
CCSP Training and Certification Prep	Yes

▼ WORK ROLES

Work Role Level	Name
Primary	Database Administrator
Primary	Knowledge Manager
Primary	Security Control Assessor
Primary	Data Analyst


IS RBT
IS-RBTI
Formal place of RECORD
DATA Collection
Create MAPPINGS
Take INVENTORY
Assess KNOWLEDGE
Intelligible DATA
Analyze DATA
Completed TRAINING PLAN


IS RBT
IS-RBTI
Formal place of RECORD
Assess KNOWLEDGE
Completed TRAINING PLAN
Analyze DATA
DATA Collection
Create MAPPINGS
Take INVENTORY
Intelligible DATA

Assess knowledge

How do we know what staff need?

Baseline Knowledge Assessment

Discern if staff have the foundational knowledge a cybersecurity professional should have.

Designed around 7 categories of NICE Framework

Assessment Questions

After reviewing the DHCP configuration, you see the following entry:

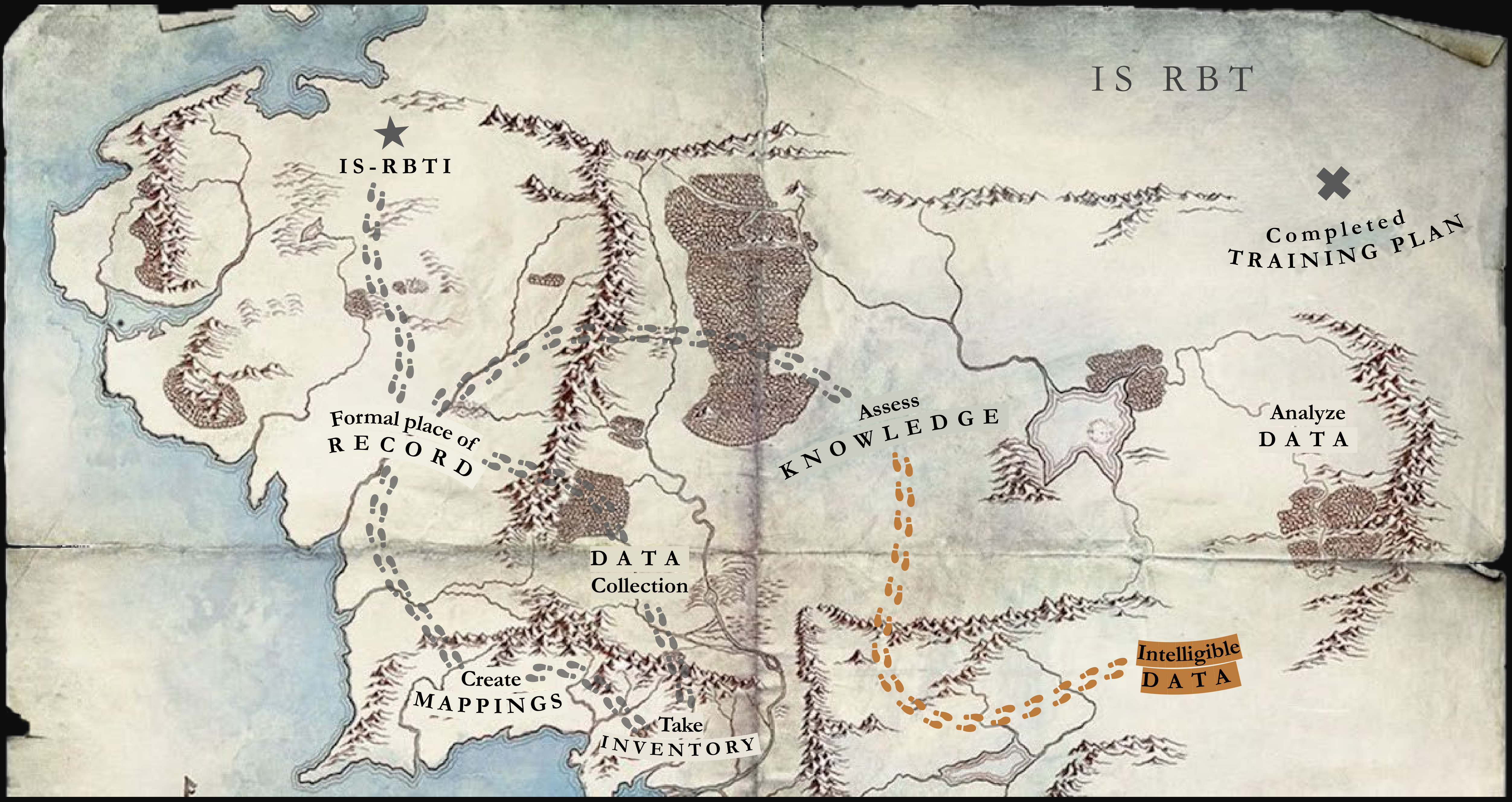
```
host relay1 {
option host-name
"smtphost1.mysite.com";
hardware ethernet
8A:00:83:AC:C0:31 fixed
address 10.130.22.01
}
```

What type of server is likely shown?

- Database server
- **I don't know**
- Web server
- Active Directory server
- Email server

+69 more

IS RBT


IS-RBTI
Formal place of RECORD
DATA Collection
Create MAPPINGS
Take INVENTORY
Assess KNOWLEDGE
Intelligible DATA
Analyze DATA
Completed TRAINING PLAN

IS RBT

IS-RBTI

Completed TRAINING PLAN

Formal place of RECORD

Assess KNOWLEDGE

Analyze DATA

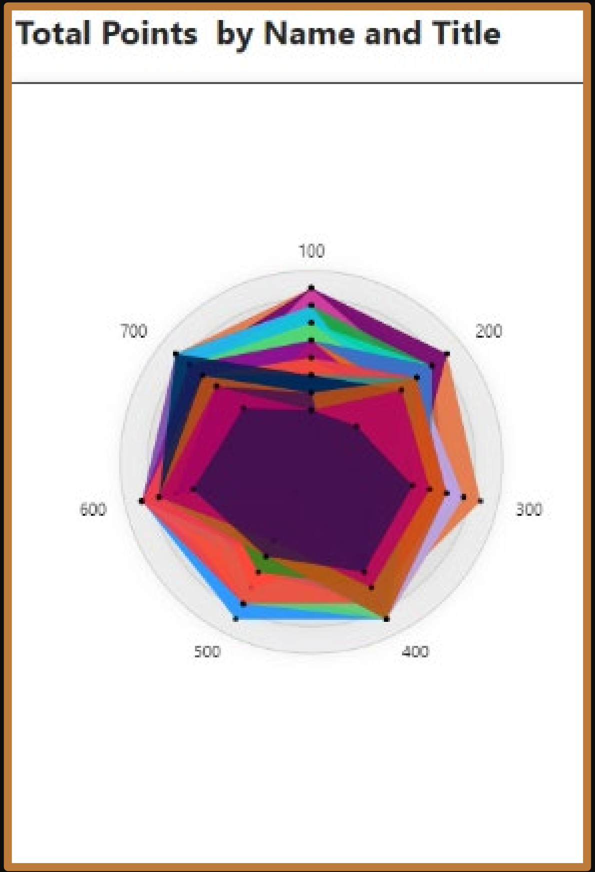
DATA Collection

Intelligible DATA

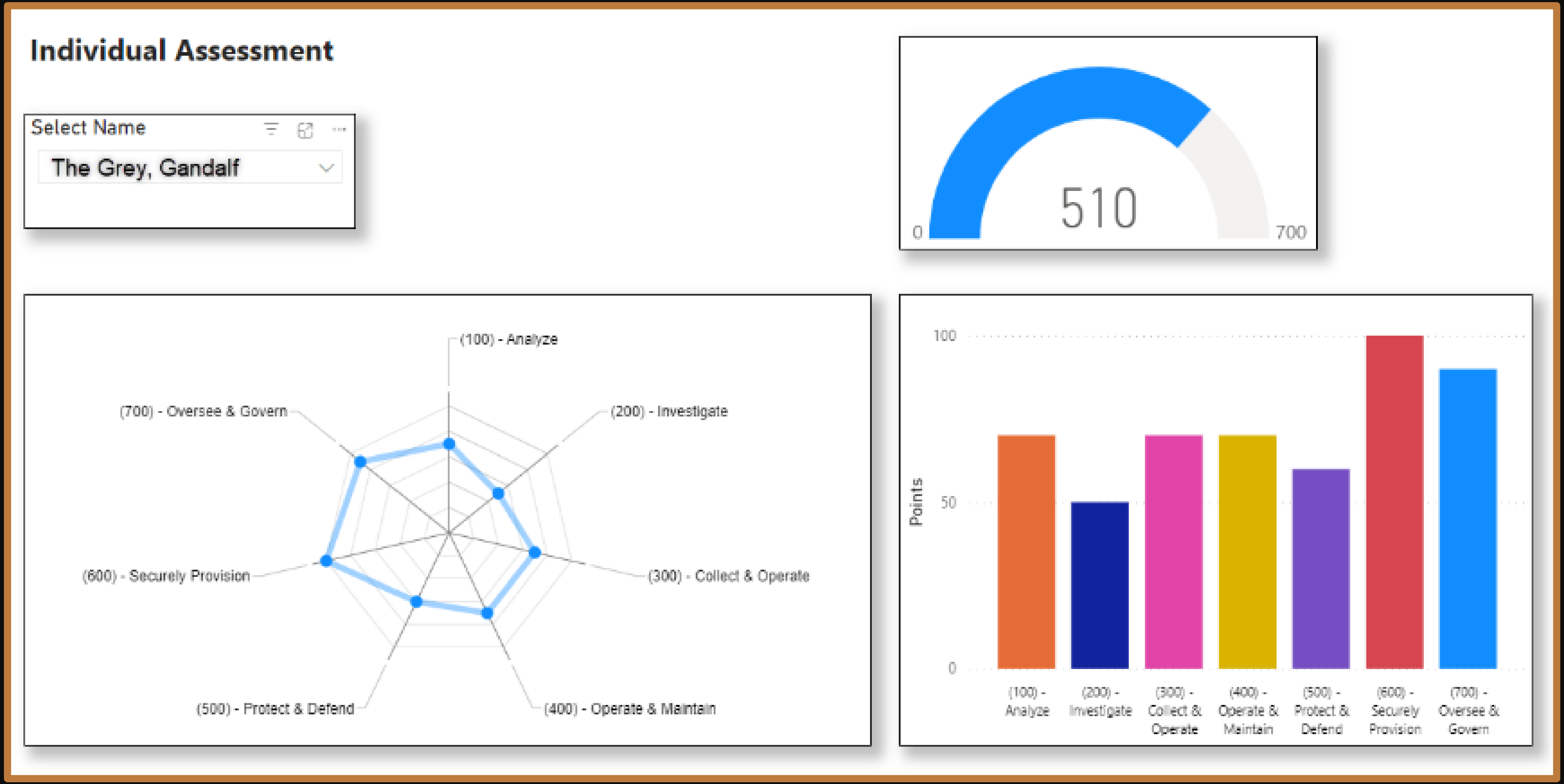
Create MAPPINGS

Take INVENTORY

Analyze results



Total Points by Name and Title

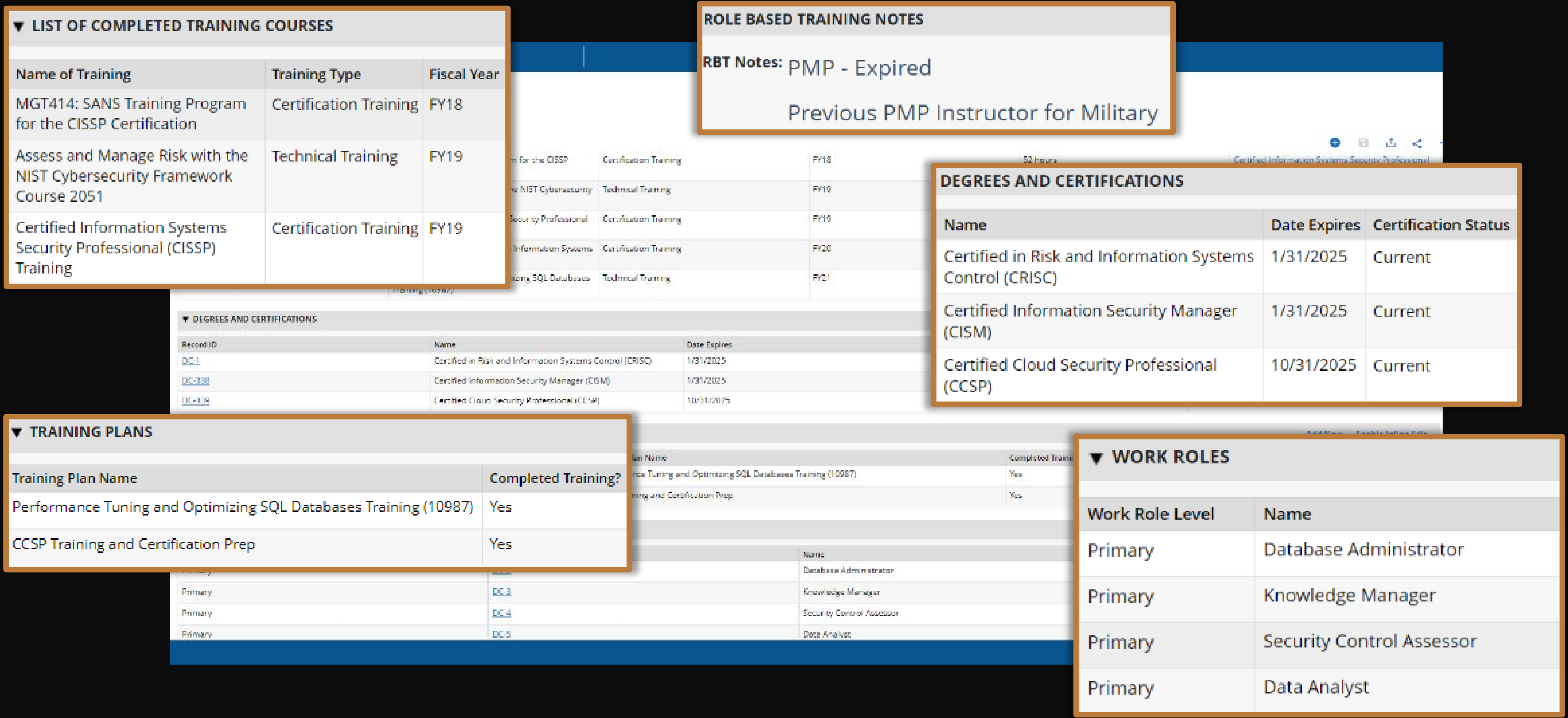


Individual Assessment

Select Name

The Grey, Gandalf

Formal place of record



▼ LIST OF COMPLETED TRAINING COURSES

Name of Training	Training Type	Fiscal Year
MGT414: SANS Training Program for the CISSP Certification	Certification Training	FY18
Assess and Manage Risk with the NIST Cybersecurity Framework Course 2051	Technical Training	FY19
Certified Information Systems Security Professional (CISSP) Training	Certification Training	FY19

ROLE BASED TRAINING NOTES

RBT Notes: PMP - Expired

Previous PMP Instructor for Military

DEGREES AND CERTIFICATIONS

Name	Date Expires	Certification Status
Certified in Risk and Information Systems Control (CRISC)	1/31/2025	Current
Certified Information Security Manager (CISM)	1/31/2025	Current
Certified Cloud Security Professional (CCSP)	10/31/2025	Current

▼ TRAINING PLANS

Training Plan Name	Completed Training?
Performance Tuning and Optimizing SQL Databases Training (10987)	Yes
CCSP Training and Certification Prep	Yes

▼ WORK ROLES

Work Role Level	Name
Primary	Database Administrator
Primary	Knowledge Manager
Primary	Security Control Assessor
Primary	Data Analyst

IS RBT

IS-RBTI

Formal place of RECORD

DATA Collection

Create MAPPINGS

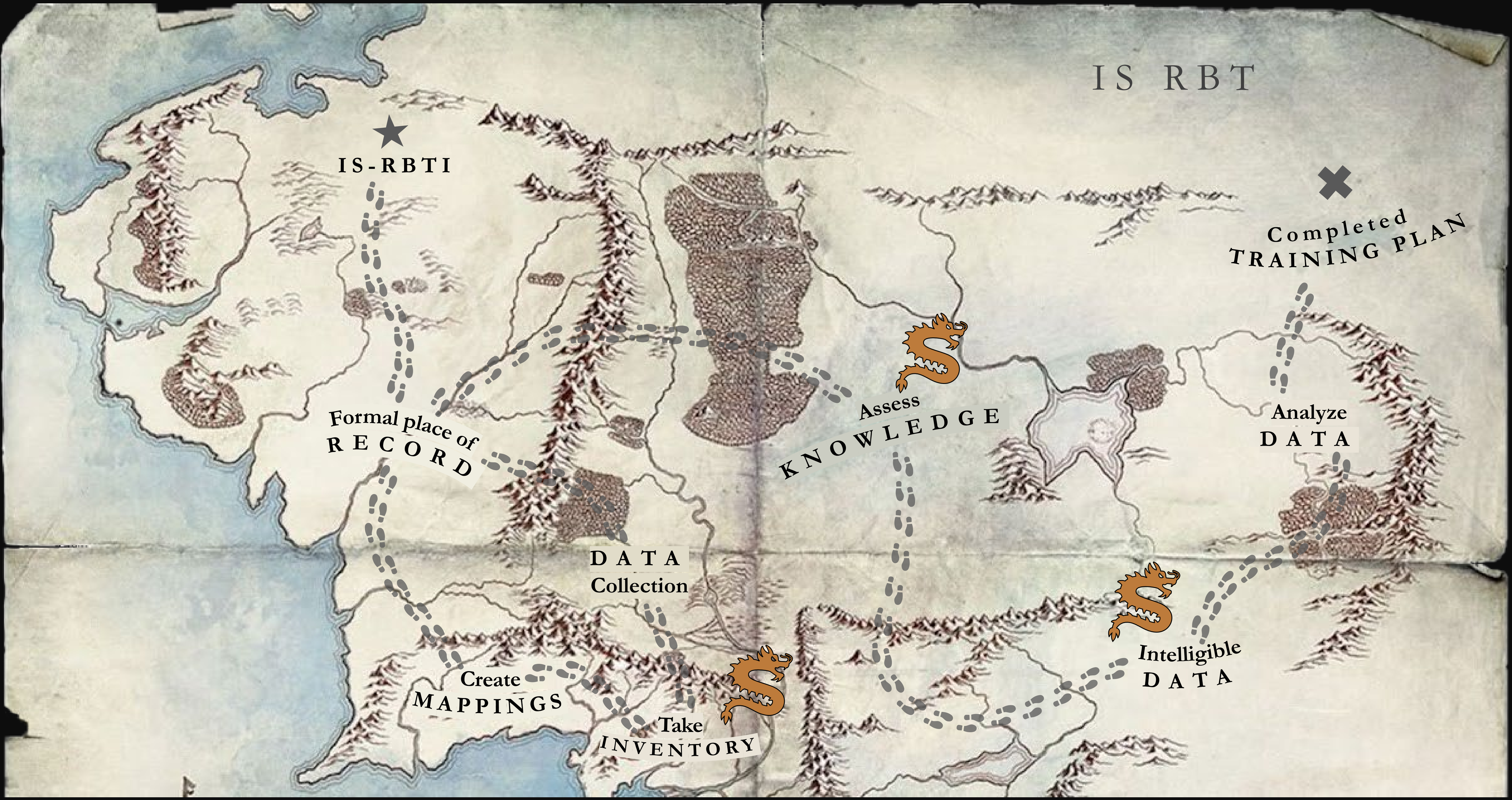
Take INVENTORY

Assess KNOWLEDGE

Intelligible DATA

Analyze DATA

Completed TRAINING PLAN


IS RBT
IS-RBTI
Formal place of RECORD
DATA Collection
Create MAPPINGS
Take INVENTORY
Assess KNOWLEDGE
Intelligible DATA
Analyze DATA
Completed TRAINING PLAN

Securing insecurities

Leadership Agreement

Results only for training

Staff Acknowledgement

Written acknowledgement

Staff Reassurance

Pre-assessment communication in meeting and email

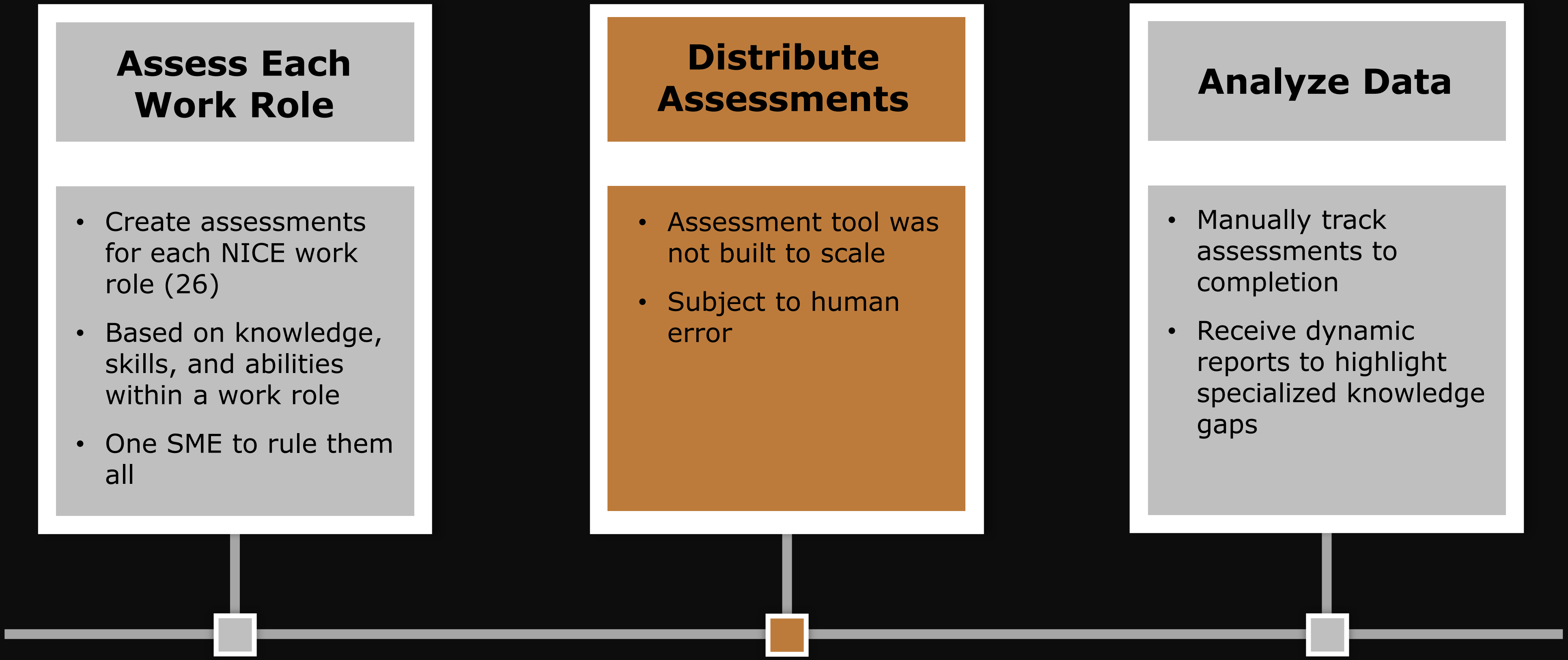
Year one conclusion

- Information repository for certifications, mappings, training plans and completed trainings
- Data on foundation knowledge gaps
- Data-driven decisions on training needs

THE DESOLATION OF THE GAP

YEAR TWO

Identifying the Gap



Assess Each Work Role

- Create assessments for each NICE work role (26)
- Based on knowledge, skills, and abilities within a work role
- One SME to rule them all

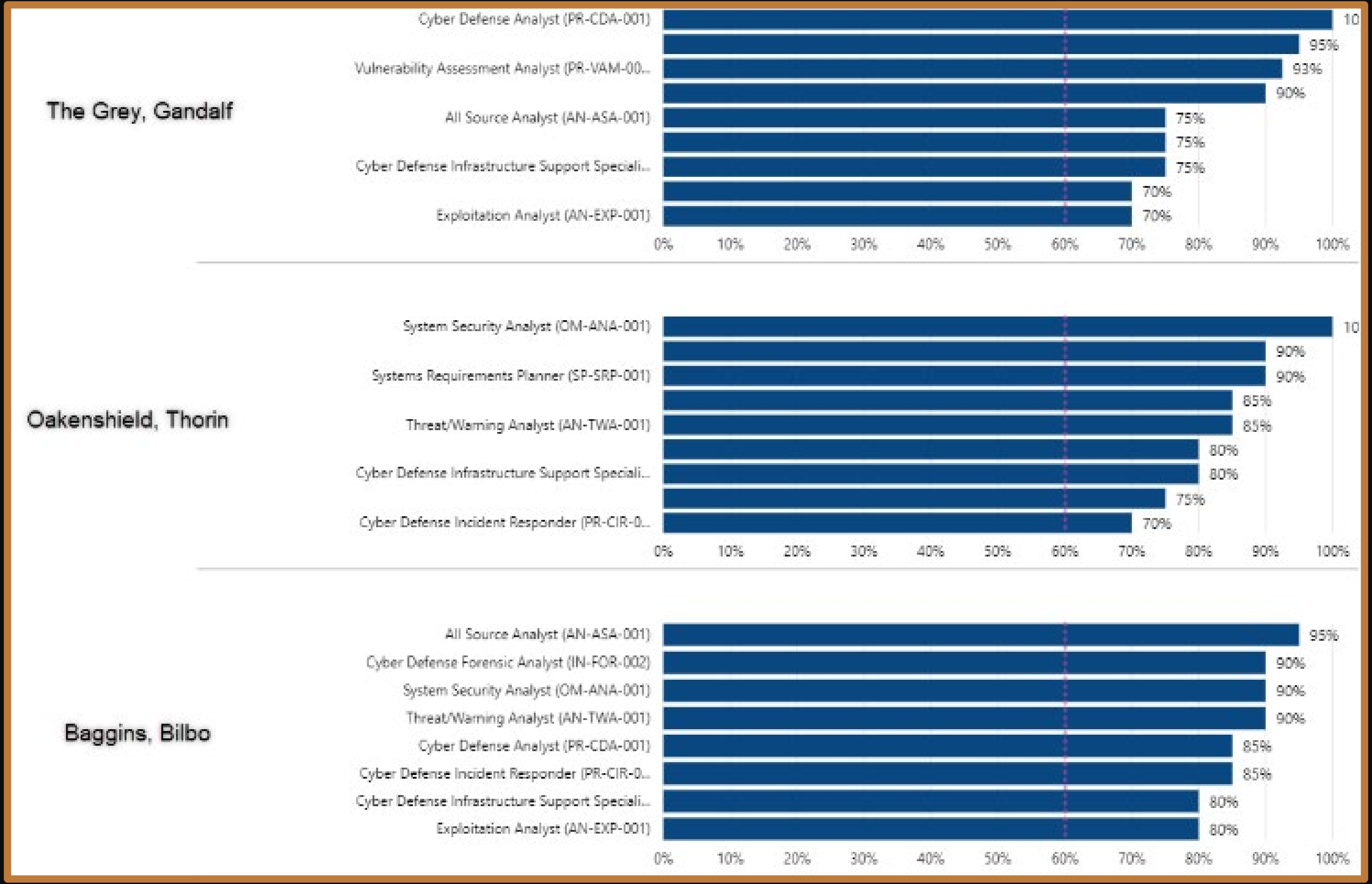
Distribute Assessments

- Assessment tool was not built to scale
- Subject to human error

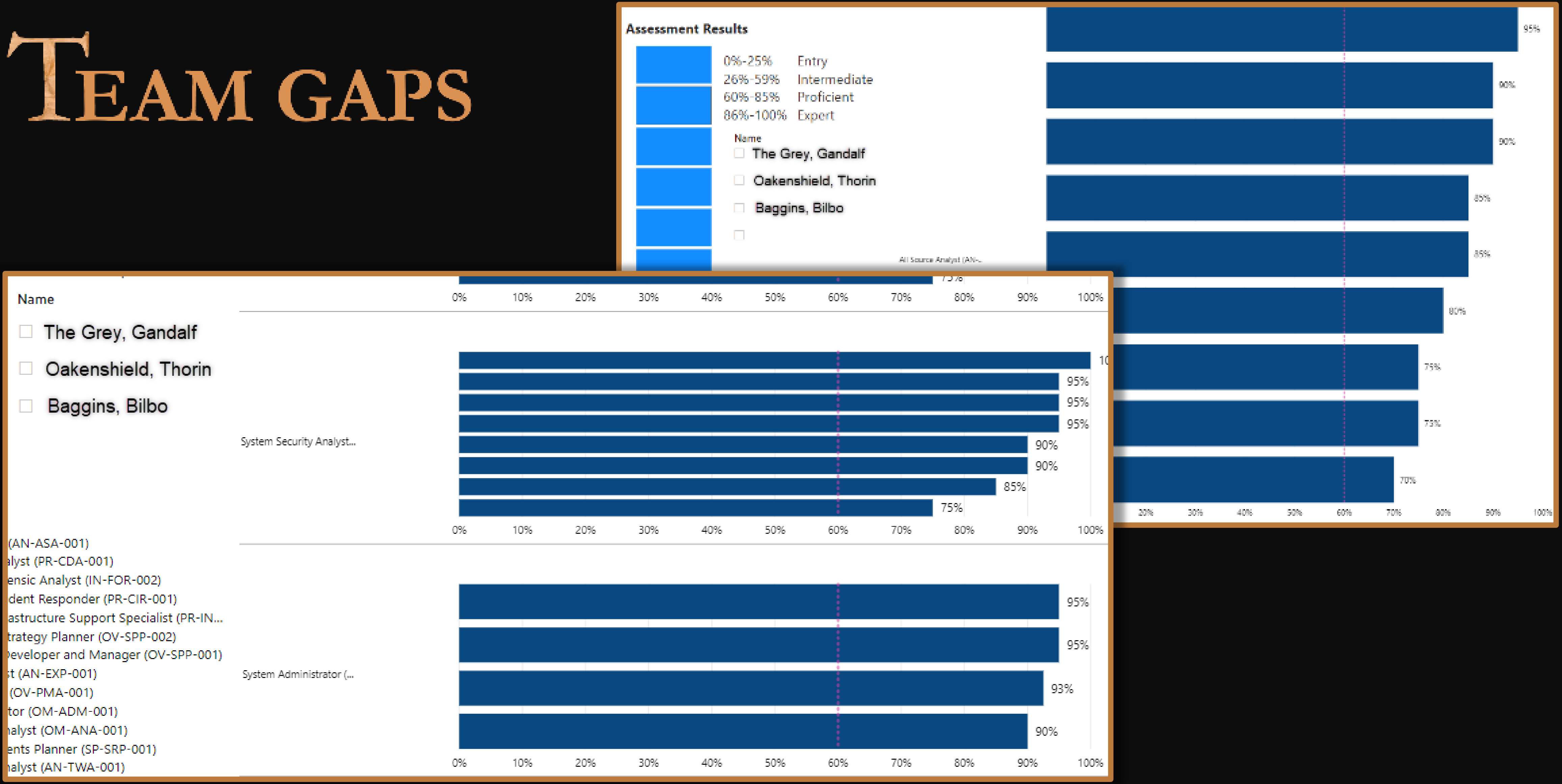
Analyze Data

- Manually track assessments to completion
- Receive dynamic reports to highlight specialized knowledge gaps

Individual gaps



TEAM GAPS



Assessment Results

🟦	0%-25%	Entry
🟦	26%-59%	Intermediate
🟦	60%-85%	Proficient
🟦	86%-100%	Expert

Name

□ The Grey, Gandalf

□ Oakenshield, Thorin

□ Baggins, Bilbo

□

Name

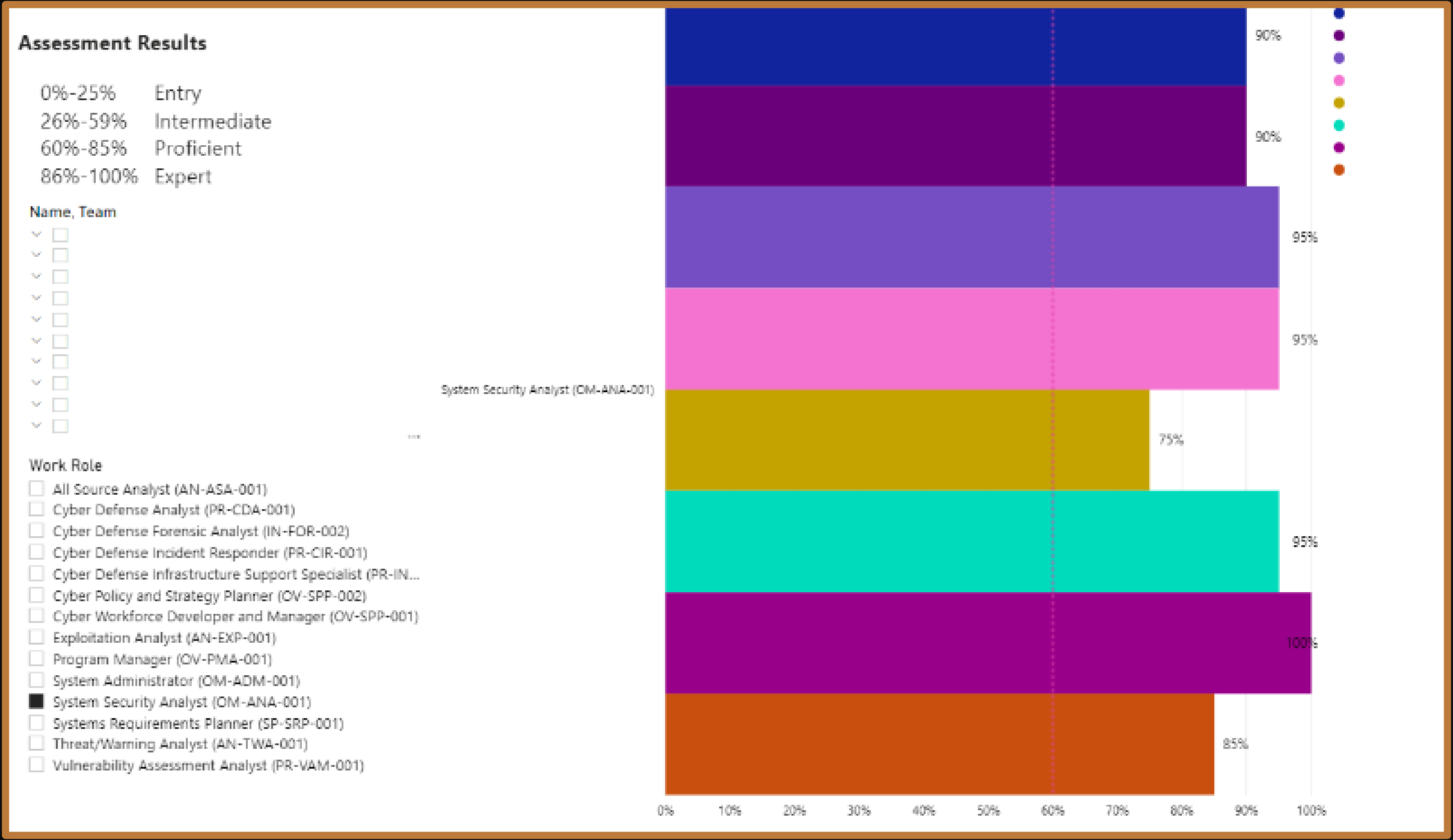
□ The Grey, Gandalf

□ Oakenshield, Thorin

□ Baggins, Bilbo

(AN-ASA-001)
alyst (PR-CDA-001)
ensic Analyst (IN-FOR-002)
dent Responder (PR-CIR-001)
astructure Support Specialist (PR-IN...
trategy Planner (OV-SPP-002)
Developer and Manager (OV-SPP-001)
t (AN-EXP-001)
(OV-PMA-001)
tor (OM-ADM-001)
alyst (OM-ANA-001)
ents Planner (SP-SRP-001)
alyst (AN-TWA-001)

Division-wide gaps



Assessment Results

0%-25%	Entry
26%-59%	Intermediate
60%-85%	Proficient
86%-100%	Expert

Name, Team

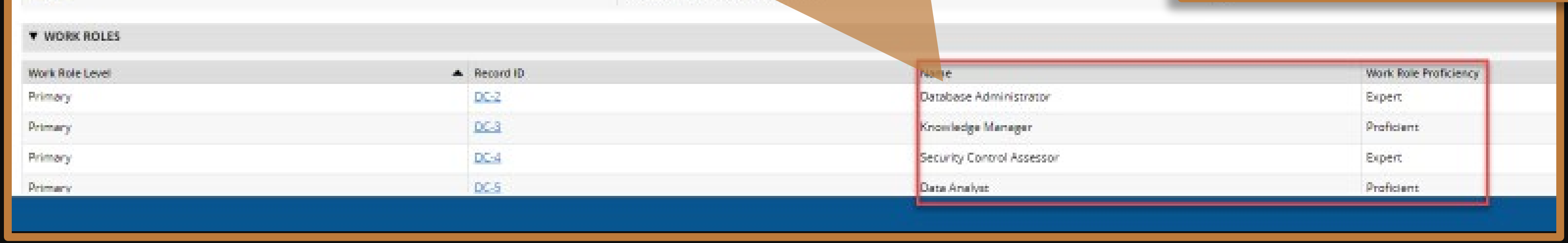
- ⌄ □
- ⌄ □
- ⌄ □
- ⌄ □
- ⌄ □
- ⌄ □
- ⌄ □
- ⌄ □
- ⌄ □
- ⌄ □

Work Role

- □ All Source Analyst (AN-ASA-001)
- □ Cyber Defense Analyst (PR-CDA-001)
- □ Cyber Defense Forensic Analyst (IN-FOR-002)
- □ Cyber Defense Incident Responder (PR-CIR-001)
- □ Cyber Defense Infrastructure Support Specialist (PR-IN...
- □ Cyber Policy and Strategy Planner (OV-SPP-002)
- □ Cyber Workforce Developer and Manager (OV-SPP-001)
- □ Exploitation Analyst (AN-EXP-001)
- □ Program Manager (OV-PMA-001)
- □ System Administrator (OM-ADM-001)
- ■ System Security Analyst (OM-ANA-001)
- □ Systems Requirements Planner (SP-SRP-001)
- □ Threat/Warning Analyst (AN-TWA-001)
- □ Vulnerability Assessment Analyst (PR-VAM-001)

Proficiency levels

Name	Work Role Proficiency
Database Administrator	Expert
Knowledge Manager	Proficient
Security Control Assessor	Expert
Data Analyst	Proficient

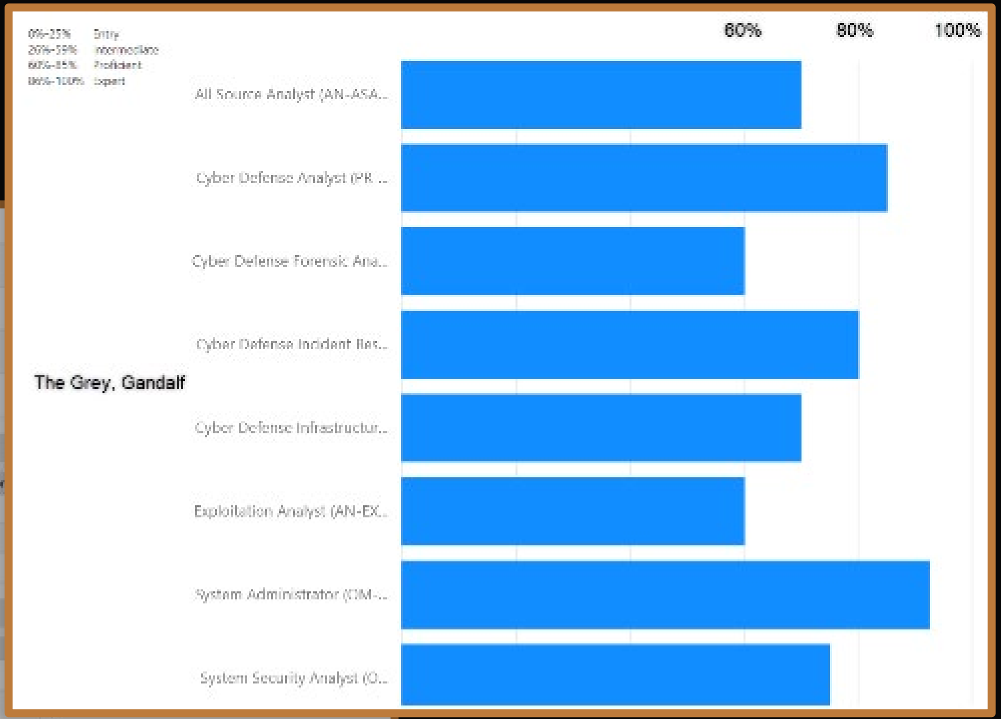


TR-00019	MGT414: SANS Training Program for the CISSP Certification	Certification Training	FY18
TR-00014	Assess and Manage Risk with the NIST Cybersecurity	Technical Training	FY19
TP-63		CCSP Training and Certification Prep	

Certification
Current
Current
Current

▼ WORK ROLES

Work Role Level ▲	Record ID	Name	Work Role Proficiency
Primary	DC-2	Database Administrator	Expert
Primary	DC-3	Knowledge Manager	Proficient
Primary	DC-4	Security Control Assessor	Expert
Primary	DC-5	Data Analyst	Proficient



0%-25%	Entry
26%-59%	Intermediate
60%-85%	Proficient
86%-100%	Expert

YEAR TWO CONCLUSION

Had a snapshot of training, certs., work-role, and proficiencies to make data-driven decisions to fill the gaps

THE BATTLE FOR KNOWLEDGE

YEAR THREE

Woes and Triumphs

The Fellowship of Review

Received feedback that assessments were poorly worded, vague, unapplicable

Triumph: Created a review board of instructors to evaluate assessments for accuracy and industry changes. Created focused assessments based on feedback from the review board.

Foundation-level Assessments

Specialized assessments were still foundational at their core

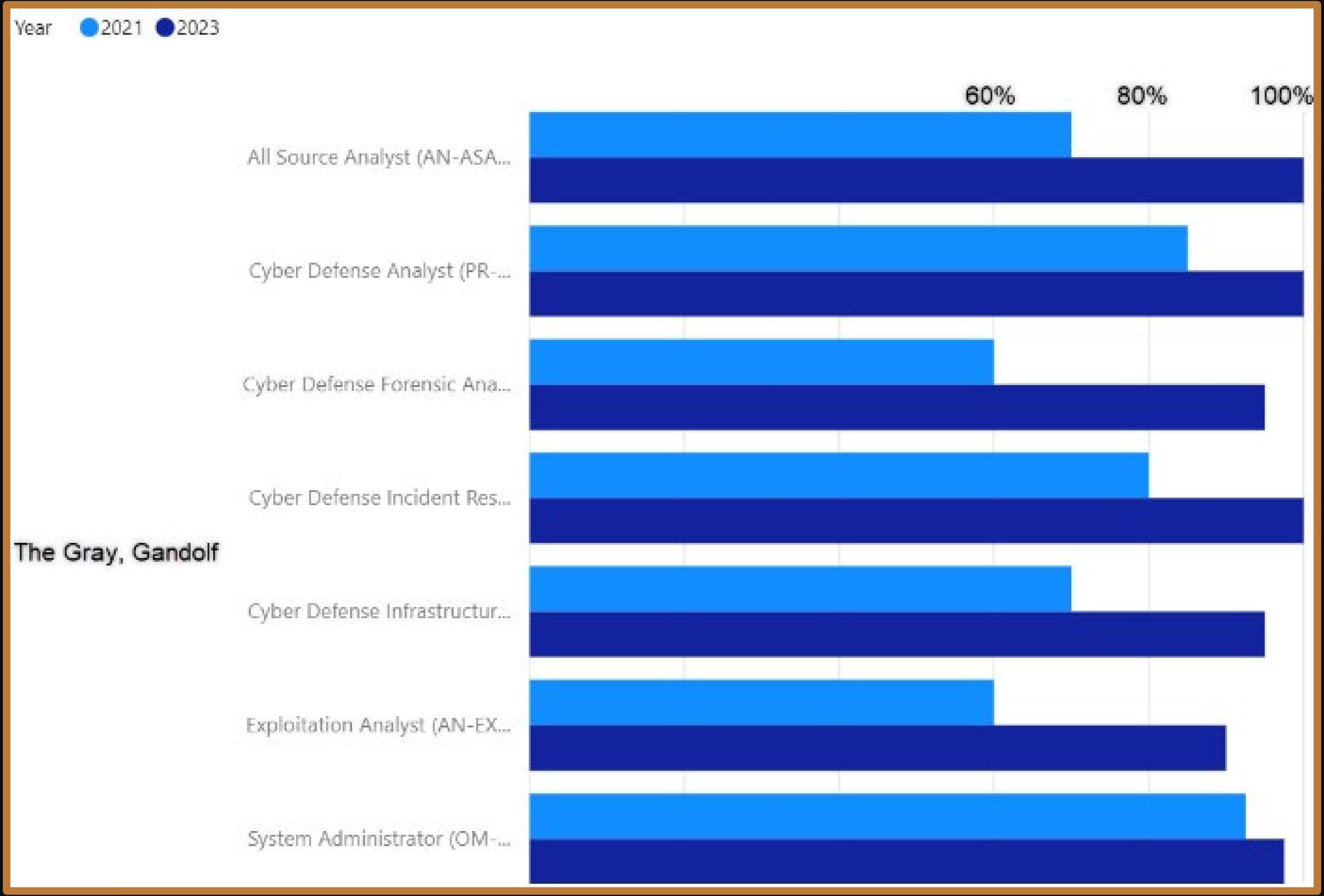
Triumph: Engaged review board again to take assessments to the next level. Also created an internal review board to ensure buy-in.

Human Error

Single-handedly checking and balancing the current platform

Triumph: Vendor created a new platform that eliminated the need for eagle-eye tracking. Distribution of assessments was much simpler.

Comparative data



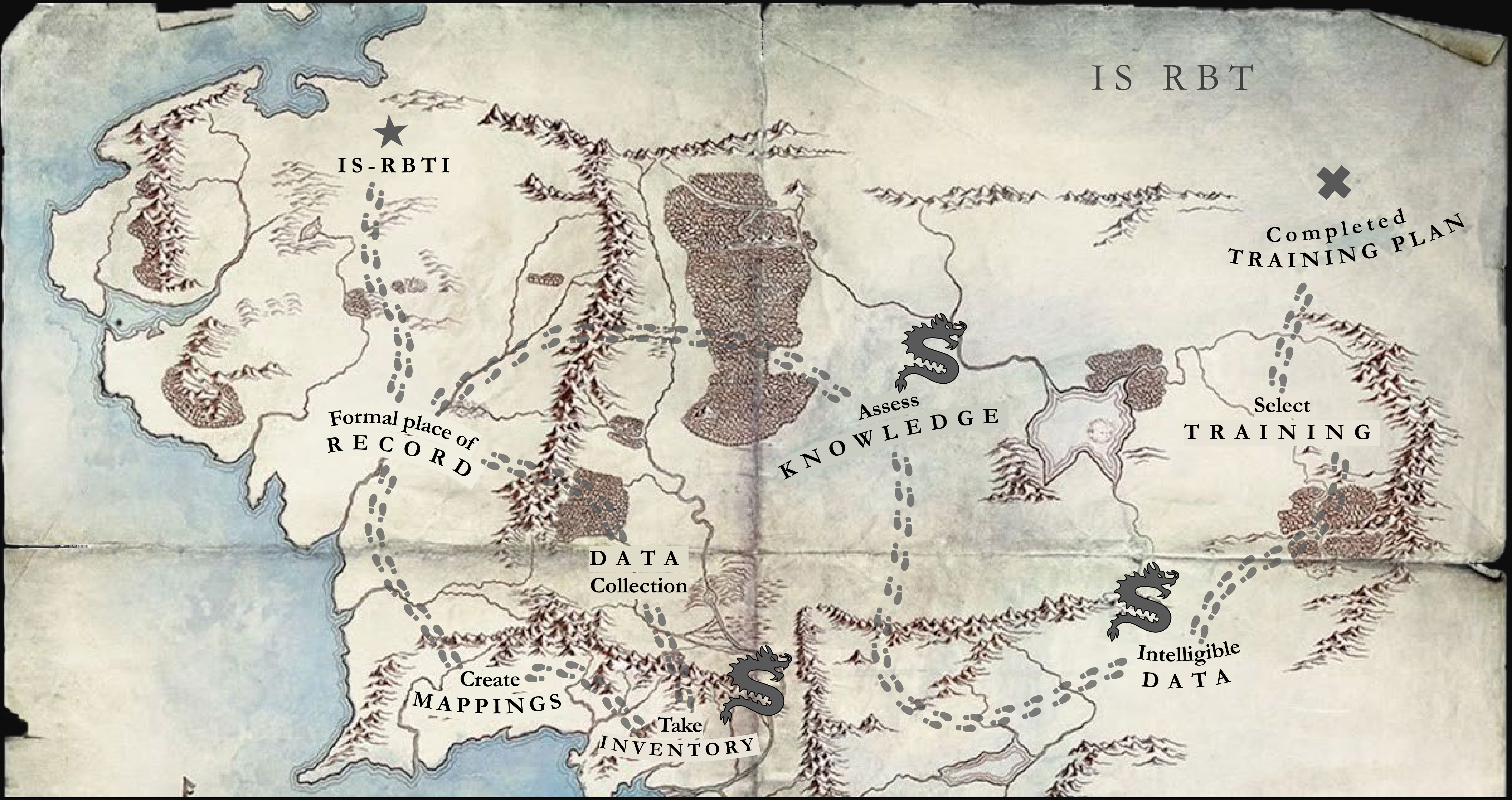
The journey continues

- Data to support the program
- A platform to support scaling and lower human error
- A path to a more advanced program

In retrospect

A DIFFERENT APPROACH

IS RBT



IS-RBTI

Formal place of RECORD

DATA Collection

Take INVENTORY

Create MAPPINGS

Assess KNOWLEDGE

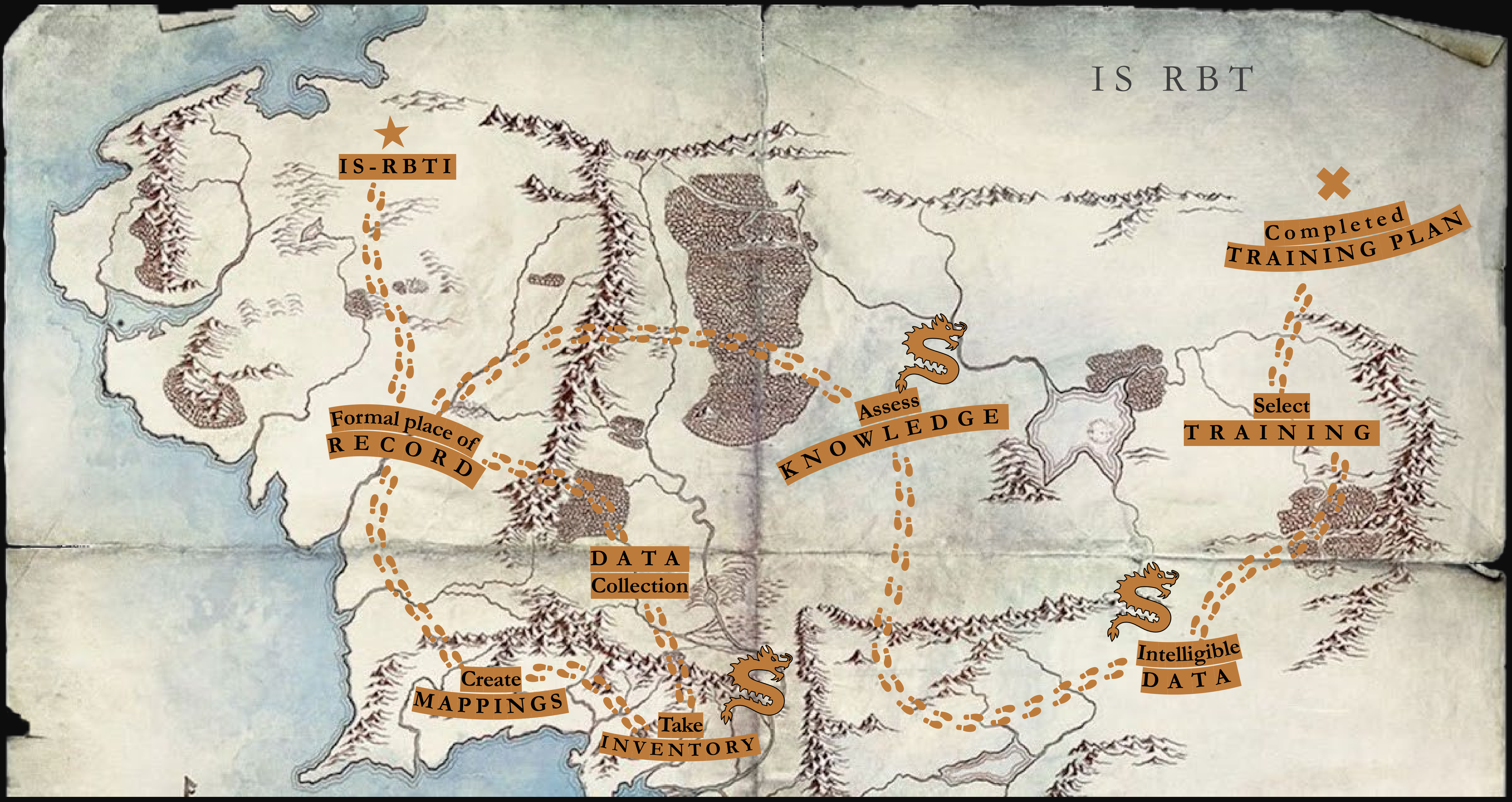
Intelligible DATA

Select TRAINING

Completed TRAINING PLAN

mal P
C
IS
G
RA
K
A
llection
date
NGS

IS RBT



IS-RBTI

Formal place of RECORD

Create MAPPINGS

Take INVENTORY

DATA Collection

Assess KNOWLEDGE

Intelligible DATA

Select TRAINING

Completed TRAINING PLAN

A DIFFERENT APPROACH

Fully realize the vision

- Don’t rush the process
- Pick the plan apart

A DIFFERENT APPROACH

Fully realize the vision

- Don’t rush the process
- Pick the plan apart

Create a program charter

- Gain leadership buy-in, new perspectives, and alternate routes
- Memorialize program existence and importance

A DIFFERENT APPROACH

Fully realize the vision

- Don’t rush the process
- Pick the plan apart

Create a program charter

- Gain leadership buy-in, new perspectives, and alternate routes
- Memorialize program existence and importance

Become friends with Excel

- Tables in Word are not easily manipulated
- Easy upkeep and reviews with pivot tables

A DIFFERENT APPROACH

Fully realize the vision

- Don’t rush the process
- Pick the plan apart

Create a program charter

- Gain leadership buy-in, new perspectives, and alternate routes
- Memorialize program existence and importance

Become friends with Excel

- Tables in Word are not easily manipulated
- Easy upkeep and reviews with pivot tables

Lean into the team

- Build a support group
- Knowledge-share with others

RESOURCES

- NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES (NICCS) WORKFORCE DEVELOPMENT
- Texas Government Code 2054.575 (3), (4), (5)
- NIST Special Publication 800-181 revision 1, the *Workforce Framework for Cybersecurity (NICE Framework)*
- Federal Virtual Training Environment (FedVTE)

Q & A

FISSEA Closing Remarks

Menachem Goldstein
FISSEA Co-Chair

fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

#FISSEA2023

Get Involved

✉ Subscribe to the FISSEA Mailing List
FISSEAUpdates@list.nist.gov

Volunteer for the Planning Committee

Serve on the Contest or Award Committees for 2024
Email fissea@list.nist.gov

Submit a presentation proposal for a future FISSEA Forum
https://www.surveymonkey.com/r/fisseacallforpresentations

FISSEA Fall Forum

November 14, 2023

1:00pm – 4:00pm ET

REGISTER TODAY: nist.gov/fissea

fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

#FISSEA2023

SAVE THE DATE

Federal Information Security Educators (FISSEA) Conference

May 14-15, 2024

Location: *National Capital Region*

#FISSEA2023 | nist.gov/fissea

fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Thank You for Attending the FISSEA Summer Forum!

fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

#FISSEA2023