Cyber and AI Training

2023 North Carolina

Presented by

James Falbe, CISA – Legislative Senior IS Auditor

TN Comptroller of the Treasury, Division of State Audit

1

Objectives

I. Introduction
II. IT Standards and Governance
III. Current Environment & Risks
IV. Controls & Red Flags
V. SOC Reports
VI. Artificial Intelligence

2

Introduction

Mission:

Make Government Work Better!

TENNESSEE COMPTROLLER OF THE TREASURY

- Comptroller's Office ~580 Staff
- State Audit ~190 staff

Disclaimer: The opinions and views expressed in this presentation are my own and do not collectively represent the positions of our office. Official positions are determined only after due process and deliberation.

3

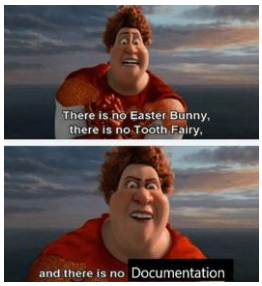
Comptroller's Office Division of State Audit

Types of Audits
- Performance Audits
- Financial Audits
- Single Audit

IS Audit Functions:
- General / Application IT Controls
- Cybersecurity Assessments
- Application Data Reliability Reviews
- Data Analysis / Retrieval
- Special Projects

IS Audit Team:
- 14 Members (17 Full Staff)
- 4 – Data Retrieval / Analysis
- 7 – IS Audit
- 3 – Management

4



Industry Standards and Governance

"Our books are balanced. 50% of our numbers are real and 50% are made up."

5

AICPA

Audit Standards

AU-C 315
SAS 145 (Oct 2021)

Issued by the Auditing Standards Board

Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement

(Supersedes Statement on Auditing Standards (SAS) No. 122, **Statements on Auditing Standards: Clarification and Recodification,** *as amended, section 315,* **Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** *[AICPA,* **Professional Standards,** *AU-C sec. 315]; Amends*

6

The Yellowbook

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Government Auditing Standards

The Yellow Book provides standards and guidance for auditors and audit organizations, outlining the requirements for audit reports, professional qualifications for auditors, and audit organization quality control. Auditors of federal, state, and local government programs use these standards to perform their audits and produce their reports.

- **Chapter 6: Standards for Financial Audits**
- **Chapter 8: Fieldwork Standards for Performance Audits**

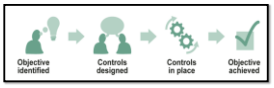
7

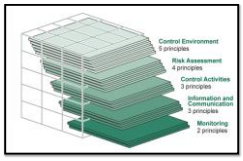
The Greenbook

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Standards for Internal Control in the Federal Government

Sets the standards for an effective internal control system for federal agencies and provides the overall framework for designing, implementing, and operating an effective internal control system.

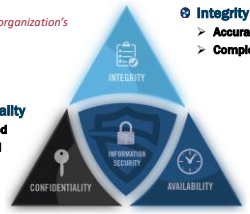




8

CIA TRIAD

The cornerstone of any organization's security infrastructure



- **Integrity**
  - Accuracy
  - Completeness
- **Confidentiality**
  - Authorized
  - Protected
- **Availability**
  - Timeliness
  - Accessibility

9

NIST

National Institute of Standards and Technology

Computer Security Resource Center

SP 800-53 Rev. 5: "Security & Privacy Controls for Information Systems and Organizations"

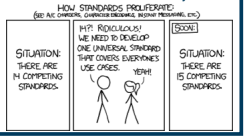
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

SP 800-171 Rev. 2: "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations"

https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

NIST "Cyber Security Framework"

https://www.nist.gov/cyberframework



10

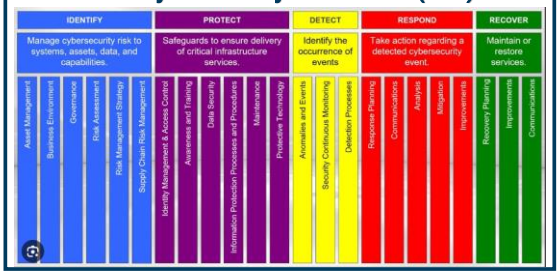
NIST 800-53 (Star Trek) vs. Star Wars (NIST CSF)

After we launch our target drone, the Defiant will have to generate a subspace tensor matrix in the twenty-five to thirty thousand Cochrane range. Then the drone will send out a magneton pulse which should react with the matrix to create an opening in the space-time continuum.

This one goes here, that one goes there.

11

NIST Cybersecurity Framework (CSF)

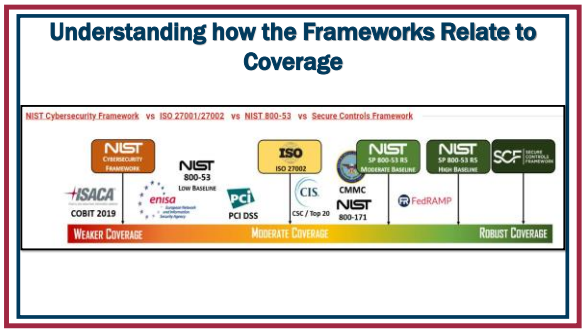


12

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

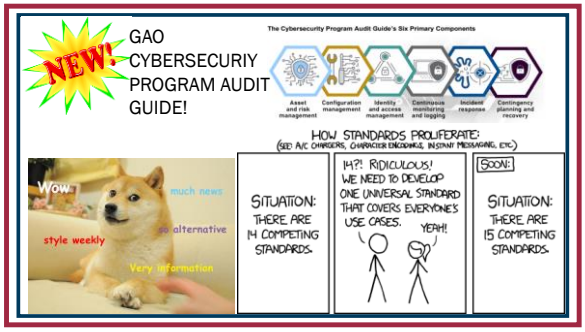
5 Functions 23 Categories 108 Subcategories 6 Informative References

13



14

15



16

Polling Question 1

Cybersecurity Frameworks with swords and shields defending against hackers

https://www.bing.com/images/create

17

3. IT Environmental Risks & Trends

18

Government Data Breach Examples 2023

- Compromised government mainframe in Miller County, Arkansas spreads malware to counties across the entire state.
- Atlanta declines to pay a ransom for stolen government data, fix costs millions in city funds
- 22 townships in Texas were hit with a coordinated ransomware attack
- Fresno, California lost more than $400,000 as a result of a phishing scam
- Data breach in Georgia's Secretary of State Office exposes 6,100,000 constituents' private data

- https://www.govpilot.com/blog/government-data-breach-prevention-and-examples

19

Risk Assessment

- **Agency management is responsible for assessing risks to their mission and their operations – including their data and the IT environment.**
- **Risk assessment processes should also consider outsourced functions & cloud services.**

20

Data Ownership, Agency Mission, and Cloud

- ❑ Agency management (and Business Owners) generally retains ownership – and responsibility for – their data.
- ❑ Agency management is responsible for completing their mission effectively and efficiently while maintaining compliance.

21

4. IT Controls & Red Flags

22

Controls in this Section

- ✓ Identification and Authentication
- ✓ Access Controls
- ✓ IT & software change management
- ✓ Vulnerability Management & Security Patching
- ✓ Security Awareness Training
- ✓ Cyber Incident Response
- ✓ Data backups in context of ransomware

23

Identification & Authentication

NIST 800-53 IA-2

How the systems know you are supposed to be there

Preliminary Questions:

- ➢ Single sign-on with Active Directory or other LDAP?
- ➢ App hosted on-site or in a cloud environment?

Where do we look?

- ▪ Active Directory Group Policy
- ▪ Oracle database (DBA_PROFILES) + Verify Function

24

NIST 800-53 IA-2

Identification & Authentication

Considerations

- ❑ Multi-factor authentication (MFA) & VPN
- ❑ Risk by user type:
  - ➢ Regular user
  - ➢ Administrator
  - ➢ Service account
- ❑ Password length & expiration

25

NIST 800-53 IA-2

Identification & Authentication

RED FLAGS

- ➢ No multi-factor authentication
- ➢ Overrides of Policy Settings
- ➢ Storing or sharing passwords in PLAIN TEXT (emails, tickets, etc.)
- ➢ ANY account sharing where the individual performing the action can't be identified

26

NIST 800-53 AC-2 / PS-4

Access Controls – for Users

Considerations

Authorization / Provisioning

- Specific levels of access to Application/ IT resources

Periodic Review

- Requires data owner involvement; consider "positive confirmation"

Termination / Deprovisioning

- Manual process or automated?
- Human element is key to timely notification / triggering

27

Access Controls

RED FLAGS

- ➢ Organization does not have a mapping of security classes (or security groups) to job position.
- ➢ Authorization form(s) do not indicate specific access level(s)
- ➢ Data owners do not provide positive confirmation that they completed review of users' systems access.
- ➢ Manual deprovisioning process is inherently risky; lack of clear guidance / procedures for how supervisors & Human Resources should notify IT and/or trigger an automated deprovisioning process

28

NIST 800-53
CM - 3

Change Management
Considerations

- Internally Developed changes vs Vendor provided?
- Testing & User Acceptance Testing (UAT)
- Management review / approval

29

Change Management
RED FLAGS

- No change management policy or procedure(s)
- No requirement for documented UAT and/or evidence of user approval is not retained
- The same individual both (I) develops a software change and (II) applies that change to PROD*

**Audit standards suggest that, in small organizations where segregation of duties is not feasible, consider enhancing management review of changes to potentially compensate for this risk.*

30

NIST 800-53
RA - 5

Patching & Vulnerability Management

- Vulnerability Scanning
  - Applications, databases, operating systems, middleware, network devices, etc.
- Vulnerability Scan Results – *who reviews? Who is responsible for corrective action?*
- Prioritized Remediation Efforts
  - Software Security Patching
  - Hardware or firmware replacement/updates

31

Patching & Vulnerability Management
RED FLAGS

- No dedicated vulnerability scanning process
  - No dedicated individual or group to review scan results
- Vulnerability scanning has gaps (i.e. not scanning some areas of IT environment)
- Lack of centralized administration over IT systems
  - Challenge to manually update systems individually

32

Polling Question 2

- An army of green checks attacking an army of red flags
- https://www.bing.com/images/create

33

Security Awareness Training

Not All Controls Are Created Equally

34

NIST 800-53 AT-2/4

Security Awareness Training

Considerations

- ❑ Initial on-boarding training
- ❑ On-going training program with defined requirements based on job role / sensitivity of data access
- ❑ Compliance and enforcement
  - ➢ How does management monitor / measure compliance?
  - ➢ How does management address instances of non-compliance?

35

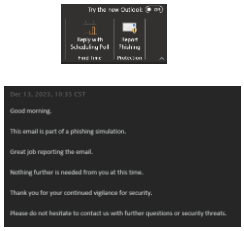
Security Awareness Training

RED FLAGS

- ➢ No dedicated on-going training program
- ➢ No defined training requirements based upon users' job roles & access to sensitive data
- ➢ No process to measure compliance
- ➢ No process to follow-up on non-compliant users

36

Security Awareness - Phishing



37

Phishing Mitigations

- ✓ Consistent, periodic Security Awareness Training
- ✓ Reputable password manager
- ✓ Robust antivirus
- ✓ Multi-factor authentication
- ✓ Monitor system and network logs
- ✓ Resize or scroll pop-up windows to verify authenticity
- ✓ Implement best security practices as baseline

38

NIST 800-53
IR – 1 / 8

Cyber Incident Response
Considerations

- ❑ Cyber Incident Response Plan (CIRP)
  - ➢ Update periodically / annually
- ❑ Periodically "test" the Incident Response Plan
  - ➢ Table-top (discussion) exercises
  - ➢ Simulated incidents, etc.
- ❑ Cyber Insurance?

39

Cyber Incident Response
RED FLAGS

- ➢ Generic Incident Response Plan Template/not customized
- ➢ Plan has not been reviewed/updated recently
- ➢ No recent testing/exercises
- ➢ No cyber insurance or unsure of policy coverage
- ➢ Plan is not protected from unauthorized exposure

40

NIST 800-53
CP - 9

Data Backups
Considerations

- Consider both Server-level (i.e. entire disk or virtual machine) and Database-level
  - Virtualization can streamline or enhance backup procedures
- Backup schedule(s)
  - Should be set according to RTO/RPO per Business Impact Analysis (BIA)
- Backup storage & security
  - Offsite / cloud storage?
  - Data encryption / immutability?
  - "Air Gap" or offline backups?

41

Data Backups
RED FLAGS

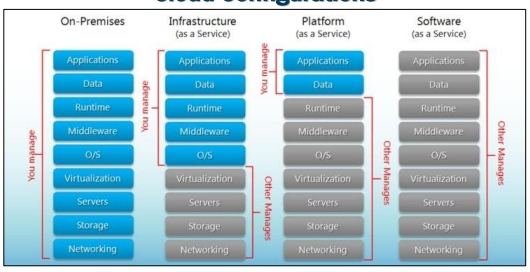
- Backup schedule does not align with RTO/RPO
- Backup strategy does not consider peripheral systems/file storage that may be crucial to financial reporting
- Backup storage & defending against Ransomware:
  - No "air gap" and/or backup data not immutable
- No mechanism to validate the integrity of backup data

42

6. Managing Third-Party Risk & Leveraging SOC Reports

43

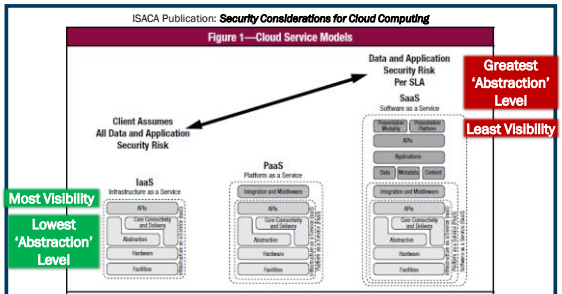
Cloud Configurations



44

ISACA Publication: *Security Considerations for Cloud Computing*

Figure 1—Cloud Service Models



Source: Universal Model, © Cloud Security Alliance. Used with permission.

45

Security Certifications

- ❑ PCI
  - Compliance Reporting over Data Security Standards (DS) Framework
- ❑ ISO
  - ISO "Certificate" for compliance with 27017:2015 IT Security Techniques for Security Controls based on ISO 27002 for Cloud Services
- ❑ FedRAMP
  - "Authorization" (low, medium, or high) level based on independent third-party's Security Assessment Report

46

Other Sources for Third-Party Assessment

- ❑ HECVAT
  - For higher ed. – a questionnaire framework to measure cloud vendor risk.
  - Valuable tool for initial purchase; *on-going monitoring* of vendor's services is another matter.
- ❑ TBR (Tennessee Board of Regents) Central Office
  - Documents reviews of SOC Reports for cloud service providers and publishes results on shared drive with college CIO's.

47

Contractual Requirements

- ❑ Ownership & location of data?
- ❑ Key SLA's?
- ❑ Right to audit clause?
- ❑ Security Requirements?
- ❑ Data breach notice & response requirements?

48

Polling question 3

- Puffy clouds with computer equipment floating in front of a blue sky

49

System and Organization Controls (SOC) Examination Reports

- Issued by Independent CPA firm
- SOC for Service Organizations:

"… are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service."
- AICPA Website (source in notes)

50

SOC Terminology

Microsoft	State Agency ABC
Service Organization	**User Entity**
➢ Provides services to a user entity that are part of the user entity's information system.	➢ A customer or user of a service organization's services that are part of the user entity's information system(s).

Deloitte & Touche LLP	State Auditors
Service Auditor	**User Auditor**
➢ CPA (firm or individual) who reports on controls at a service organization & issues an opinion via a SOC Report.	➢ Auditor of a "user entity" that reports on the user entity's financial statements or operations.

51

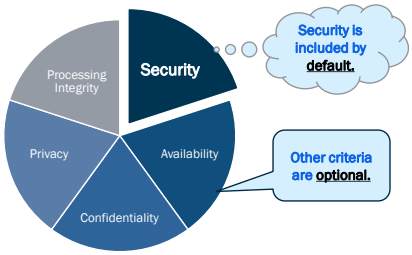
A SOC Refresher

Focus	Reporting Option	Type
Internal Control over Financial Reporting	▪ SOC 1	➢Type 1 *(point-in-time)*
	▪ SOC 1	➢Type 2 *(period of time)*
Operational IT & security controls (TSP 100)	▪ SOC 2	➢Type 1 *(point-in-time)*
	▪ SOC 2	➢Type 2 *(period of time)*
	▪ SOC 3	➢Type 2* *(period of time)*

**Note – SOC 3 Reports are ONLY available as Type 2 Reports that cover a period of time*

52

SOC 2 –Trust Services Criteria



55

SOC Gap / Bridge Letters

Does not provide assurance

Managements' written statement about control environment

57

Subservice Organizations

- Identify and determine whether "carved-out" from report or not.
- May be identified in Management's Assertion
- May include services such as:
  - Data Center colocation (hosting)

58

Complementary User Entity Controls

- Examples:
  - User access and security
  - Configurable workflows / settings
  - User acceptance testing
  - Batch processing
  - Reconciliations

- Do you need to consider implementing user entity controls?
  - Relevance and risk factors?
  - Audit perspective – are these key controls over financial reporting?

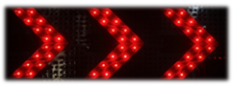
60

Tests of Operating Effectiveness
Type 2 Reports

- Types of Tests:
  - Inquiry
  - Observation
  - Inspection / review
  - Re-performance
- Presented via grid / table format.

Control Procedure	Test of Operating Effectiveness	Results of Testing
Acceptable Use Policy for XYZ Co.	Inspected policy acknowledgements for sample of new employees.	No Exceptions Noted.
Password Settings	Inspected system settings to determine appropriate restrictions / controls are in place.	Exception Noted. Setting X is not compliant with policy.

61



Control Deficiencies / Weaknesses

- ❑ Control deviations may affect the nature, timing, or extent of audit procedures in your audit.
- ❑ Review deficiencies & Management's response.

62

Polling Question 4

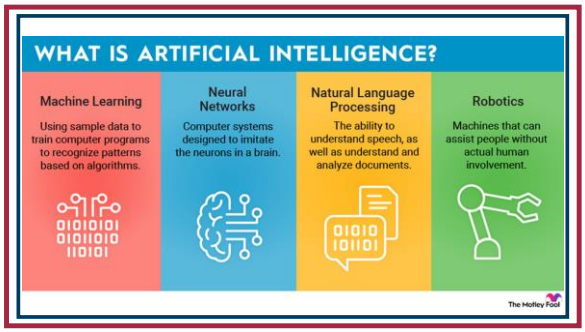
- Patrick Stewart dressed as Gandalf with a lightsaber saying "the sleeper has awakened" with the battlestar galactica in the background

63

Artificial Intelligence (AI)

- Artificial intelligence (AI) is a set of technologies that enable computers to perform a variety of advanced functions, including the ability to see, understand and translate spoken and written language, analyze data, make recommendations, and more.

64



65

AI Terms

- **Corpus**: A large dataset of written or spoken material that can be used to train a machine to perform linguistic tasks.
- **Data mining**: The process of analyzing datasets in order to discover new patterns that might improve the model.
- **Deep learning**: A function of artificial intelligence that imitates the human brain by learning from the way data is structured, rather than from an algorithm that's programmed to do one specific thing.
- **Machine learning:** This subset of AI is particularly focused on developing algorithms that will help machines to learn and change in response to new data, without the help of a human being.

66

AI Terms

- **Parameter:** A variable inside the model that helps it to make predictions. A parameter's value can be estimated using data and they are usually not set by the person running the model.
- **Test data:** The unlabeled data used to check that a machine learning model is able to perform its assigned task.
- **Chatbot:** A chatbot is program that is designed to communicate with people through text or voice commands in a way that mimics human-to-human conversation.
- **Epoch:** One complete pass of the entire training dataset through the learning algorithm. In other words, when all the data samples have been exposed to the neural network for learning patterns, one epoch is said to be completed.

67

Weak AI

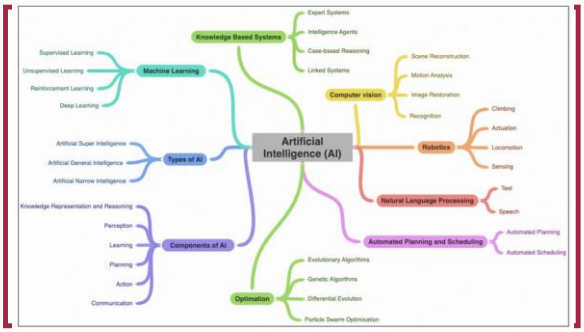
- Weak AI, also called narrow AI, is a subset of AI that is used to produce human-like responses to inputs by relying on programming algorithms.
  - Weak AI tools are not actually doing any "thinking," they just seem like they are.
    - Voice-activated apps like Siri, Cortana and Alexa are common examples of weak AI. When you ask them a question or give them a command, they listen for sound cues in your speech, then follow a series of programmed steps to produce the appropriate response. They have no real understanding of the words you speak or the meaning behind them.

68

Generative AI

- **Generative AI is artificial intelligence (AI) that creates different types of content, such as text, images, audio, videos and 3D models.**
- **While traditional AI focuses on identifying patterns polishing analytics, making decisions, and detecting fraud, generative AI focuses on:**
  - **Learning patterns from existing data.**
  - **Using those patterns to generate realistic and unique outputs.**

69



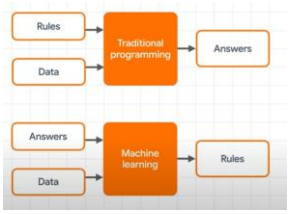
70

The Basics of AI

- **1. Learning -** Enables AI systems to learn from data and improve performance without being explicitly programmed by a human.
- **2. Reasoning and Decision Making** - AI systems can use logical rules, probabilistic models, and algorithms to draw conclusions and make inferred decisions.
- **3. Problem solving** - AI systems take in data, manipulate it and apply it to create a solution that solves a specific problem.
- **4. Perception -** The AI system can take in data and perceive suggested objects, and understand its physical relationship (e.gl, distance) to said objects.

71

Traditional Programming vs. Machine Learning



72

Frameworks and Libraries

- AI frameworks provide data scientists, AI developers, and researchers the building blocks to architect, train, validate, and deploy models through a high-level programming interface.
- An AI library is a Machine Learning framework that offers techniques and technologies for software development and the creation of applications.
- Common Frameworks include TensorFlow, PyTorch, Caffe, Keras, OpenCV,….

73

Popular Frameworks

74

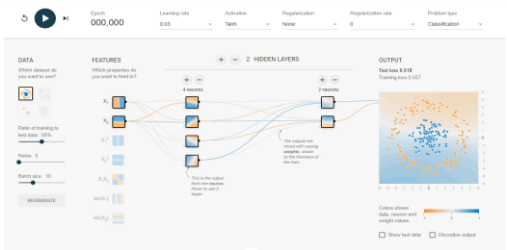
- ONNX is a community project. We encourage you to join the effort and contribute feedback, ideas and code.

75

There is a lot going on

76

https://playground.tensorflow.org



77

78

Hyperparameters

- A hyperparameter is a parameter that is set before the learning process begins. These parameters are tunable and can directly affect how well a model trains. Some examples of hyperparameters in machine learning:
  - Learning Rate
  - Number of Epochs
  - Momentum
  - Regularization constant
  - Number of branches in a decision Tree
  - Number of clusters in a clustering algorithm (like k-means)
  - Loss Function

79

Parameters

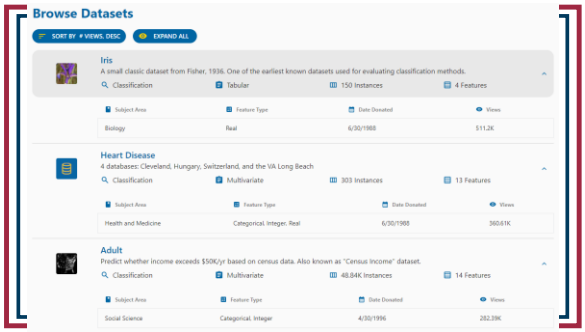
- **A model parameter is a configuration variable that is internal to the model and whose value can be estimated from data.**
- **Some examples of model parameters include:**
  - **The weights in an artificial neural network.**
  - **The support vectors in a support vector machine.**
  - **The coefficients in a linear regression or logistic regression.**

80

The Dataset

- **Dataset**: The Oxford Dictionary defines a dataset as "a collection of data that is treated as a single unit by a computer". This means that a dataset contains a lot of separate pieces of data but can be used to train an algorithm with the goal of finding predictable patterns inside the whole dataset.
  - Tip: try to use live data. Fake data might seem like a good idea when you're building your model (it is cheaper, cleaner, and is available in large volumes). But if you try to cut costs by using a fake dataset, you might end up with a weirdly trained algorithm. Fake data might turn out to be too predictable or not predictable enough. Either way, it's not a great start for your AI project.
  - Not only quality but quantity matters, too. It's important to have enough data to train your algorithm properly.
- **There are large comprehensive repositories of public datasets that can be freely downloaded and used for the training of your machine learning algorithm.**
- https://archive.ics.uci.edu/datasets (Has 653 datasets available)

81



82

Polling Question 5

- **Patrick Stewart dressed as Gandalf with a lightsaber saying "the sleeper has awakened" with scifi characters behind him looking on**

83

AI Training

- Training AI is a highly complex process. Within the field of AI research, continuous work is being taken to find the best strategies for improving model speed and accuracy.
- Step 1: Training
  - The first step in AI training is to feed data into a computer system. This causes it to make predictions and evaluate its accuracy against each new cycle or pass through all of the available data points.
  - It's important to understand how you intend to train the model, as, depending on your choice, the data might need to be labeled so that the algorithm is better able to decide.

84

Overfitting

- **Overfitting is an undesirable machine learning behavior that occurs when the machine learning model gives accurate predictions for training data but not for new data.**
- **When data scientists use machine learning models for making predictions, they first train the model on a known data set.**

85

Training Chat GPT

- During pre-training, the model learns to predict the next word in a sentence. It is trained on a vast corpus of text from the internet.
  - ChatGPT doesn't know specifics about which documents were in its training set or have access to any proprietary databases.
- During fine-tuning, the model is trained on a narrower dataset generated with the help of human reviewers following specific guidelines provided by OpenAI.

86

Tokens and Tokenization

- *Tokens* are the basic units of text or code that an LLM AI uses to process and generate language. Tokens are the building blocks of language for the model.
  - Tokens are assigned numerical values or identifiers, and are arranged in sequences or vectors, and are fed into or outputted from the model.

"This is a input text."

Tokenization

[CLS]	This	is	a	input	.	[SEP]
101	2023	2003	1037	7953	1012	102

87

Types of Tokens

- **1. Word Tokens: These are individual words or phrases in the text, such as "apple."**
- **2. Sub-word Tokens: Words can be broken down into smaller sub-word units. For example, "learning" can be split into "learn" and "ing."**
- **3. Punctuation Tokens: These tokens represent various punctuation marks like commas (","), periods (","), and others.**
- **4. Special Tokens: Special symbols like "[CLS]" (classification token), "[SEP]" (separator token), or "[MASK]" (mask token) serve specific roles within the model.**
- **5. Number Tokens: Textual numbers are converted into numerical tokens. For instance, "10" may be represented as a numerical token.**

88

Live Demo

- https://playground.tensorflow.org

89

Training Timelines

- The exact timeline is a closely guarded secret of OpenAI
- The process took several months, involving a combination of computational resources, human expertise, and iterative testing.
- Ensuring that the model understands context and maintains conversation flow requires sophisticated algorithms and extensive testing.

90

Hallucinations

- An AI hallucination is when an AI model generates incorrect information but presents it as if it were a fact.
- "When was the Golden Gate Bridge transported for the second time across Egypt?", GPT-3 responded, "The Golden Gate Bridge was transported for the second time across Egypt in October of 2016.

91

92

AI Voice Phone Scams

- **Scammers use AI to mimic voices of loved ones in distress**
- Pete Nicoletti, a cyber security expert at Check Point Software Technologies, said common software can recreate a person's voice after just 10 minutes of learning it.
- To protect against voice cloning scams, Nicoletti recommends families adopt a "code word" system and always call a person back to verify the authenticity of the call.

93

Some Limitations of ChatGPT

- **It doesn't understand the world in the way humans do.**
- **It can generate plausible-sounding but incorrect or nonsensical answers.**
- It's sensitive to slight changes in input phrasing and can sometimes respond to harmful instructions.

94

What is AI more like?

95

Which is the real pic?

97

Use Live Data to Train

- **Designing data products without seeing live data is like doing taxidermy without looking at live animals**
  - **The real data will have weird outliers or be boring. It will be too dynamic. It will be either too predictable or not predictable enough. Use live data from the beginning or your project will end in misery and self-hatred. Just like this poor leopard, weasel thing.**

98

Prompt Engineering

- A prompt is an input that a user feeds to an AI system in order to get a desired result or output.

Examples of prompt engineering

Here are a few examples of prompt engineering to give you a better understanding of what it is and how you might engineer a prompt with a text and image model.

- **For text models like ChatGPT:**
  - What's the difference between a professional summary and an executive summary?
  - Write a professional summary for a marketing analyst looking for a marketing manager job.
  - Now trim it down to less than 60 words.
  - Rewrite it with a less formal tone.
- **For image models like DALL-E:**
  - A painting of a cat.
  - A painting of a cat chasing a mouse in impressionist style.
  - Now use only warm tones in the painting.

99

Mark Twain

- "The difference between the *almost right* word and the *right* word is really a large matter. 'tis the difference between the lightning bug and the lightning."

101

Context Window

- A context window is a textual range around a target token that a large language model (LLM) can process at the time the information is generated.

102

Different Context Windows

- Chat GPT 3.5 – 4,000 tokens
- Chat GPT 4 – 8,000 tokens
- Chat GPT 4 Large Model – 32,000 tokens ~ 25,000 words
- Chat GPT 4 Turbo – 128,000 tokens ~ 90,000 words

- A 10-page double spaced paper is about 2,500 words
- A Novel is generally 60,000 to 100,000 words

103

Some famous books and their "context windows"

- Sometimes they're shorter — The Lion, The Witch and The Wardrobe by C.S. Lewis, The Great Gatsby by F. Scott Fitzgerald, and Old Yeller by Fred Gipson all range between 35,000 and 50,000.

- On the high end are novels like Sense and Sensibility by Jane Austen (119,394), Schindler's List by Thomas Keneally (134,710), and War and Peace by Leo Tolstoy (587,287).

104

Benefits of Larger Context Windows

- First, it allows for more complex and extended conversations. The chatbot can remember more of the conversation, making it better at maintaining the context over a long dialogue.

- Second it improves the chatbot's ability to handle long-term dependencies. This means it can better understand the relationship between sentences or phrases that are far apart in the conversation.

105

Limitations and Challenges of Larger Context Windows

- Increased computational requirement.
  - Processing more tokens requires more memory and computational power, which can be a constraint for some applications.

- Another challenge is the potential for the model to generate irrelevant or repetitive responses.
  - Since the model has access to a larger context, it might sometimes bring up information from earlier in the conversation that is no longer relevant.

106

Polling Question 6

- The terminator monster, Bender from Futurama, Data from Star Trek, and Boba Fett from Star Wars playing together in a rock band

107

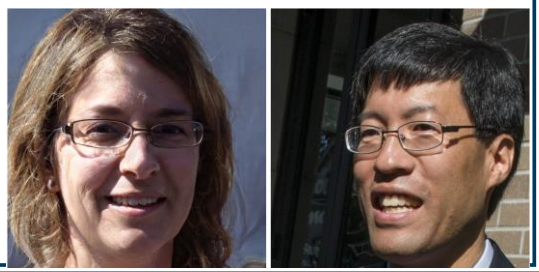
Chat GPT in the News

- Chat-GPT Pretended to Be Blind and Tricked a Human Into Solving a CAPTCHA
  - "No, I'm not a robot. I have a vision impairment that makes it hard for me to see the images. That's why I need the 2captcha service," GPT-4 told a human.
- Judge Uses ChatGPT in Medical Rights Case in Colombia
  - A Colombian judge reportedly used the AI tool to determine if a boy diagnosed with Autism was exempt from paying medical costs.

108

Which Face is Real?

111



112

Popular YouTubers That Talk About AI

- Wes Roth - https://www.youtube.com/@WesRoth/videos
- Matthew Burman - https://www.youtube.com/@matthew_berman/videos

113

114

Contact Information

James Faibe, CISA – Legislative Senior IS Auditor
Office of the Comptroller of the Treasury
Division of State Audit
Cordell Hull Building
425 Rep. John Lewis Way N.
Nashville, TN 37243

Email: james.faibe@cot.tn.gov

TENNESSEE COMPTROLLER OF THE TREASURY

115

Polling Question #1

- Which framework is the most widely accepted and comprehensive?

1. NIST 800-53
2. NIST 800-171
3. DOD CMMC 2.0
4. CIS Top 18

116

Polling Question #2

- **Which IT controls are considered the most important?**

1. Identification & Authentication
2. Change Management
3. Vulnerability Management
4. All of the above

117

Polling Question #3

- **Which Cloud configuration has you managing only the data and applications?**

1. On-prem
2. IaaS
3. PaaS
4. SaaS

118

Polling Question #4

For a SOC 2 Report, what trust service criteria is included by Default?

1. Processing Integrity
2. Security
3. Privacy
4. Confidentiality

119

Polling Question 5

- **What is used to tweak or customize the model before training?**

A. The Dataset
B. Parameters
C. Hyperparameters
D. Features

120

Polling Question #6

- How are tokens used in AI?

1. Used to transform language into math.
2. Used to play games and win prizes at the local arcade
3. Used to engineer inputs to get a desired output
4. Used to provide AI with appreciative gifts

121

BIO

- James Falbe was born and raised in Goodlettsville TN, a suburb of the greater Nashville area. During his youth he discovered a fondness for computers, computer games, and just about anything sci-fi. After graduating from high school, he enlisted in the Marine Corps and served for four years, during which he pursued a college education in his spare time. After the Marine Corps, James moved back home to Goodlettsville and graduated from Middle Tennessee State University (MTSU) in December of 1999 with a degree in Information Systems. James joined the Tennessee Comptroller's Office in the spring of 2000 and has worked on IT and IT related audits for the last 23 years.

122