



# How AI Will Impact PCI DSS Assessments in the Future

---

Presenter: Eric Sampson

# Presenter – Eric Sampson



Senior Manager



# Company Info



## Consolidated Cybersecurity Assessments

Drive quantifiable efficiencies.

Reduce the burden on your internal team.

Elevate your cybersecurity posture.

SOC | ISO | PCI | HITRUST | FedRAMP | Privacy | CMMC | Penetration Testing

[schellman.com](https://schellman.com)



# Before There Was AI...

- The invention of the printing press in 1440 put scribes out of work.
- In the 1800s, 80% of American jobs were on farms. Today, it's 2%.
- Telephone invented by Alexander Graham Bell in 1876.
- The Internet was invented in the 1970s.
- The World Wide Web was invented in 1989.
- Jobs of the future – The AI era will transform industry like we've never seen. AI has the potential to be highly disruptive in every industry.

# Gartner Survey: CEOs Predict Major AI Impact by 2026

- A recent Gartner survey of CEOs and executives found that 21% believe AI will greatly impact their industry in the next three years
- AI cited as the top disruptive technology impacting industries
- "Generative AI will profoundly impact business," said Mark Raskino of Gartner. "AI is reaching a tipping point, and CEOs fear missing out competitively."

Source: <https://www.gartner.com/en/newsroom/press-releases/2023-05-17-gartner-survey-finds-ceos-cite-ai-as-the-top-disruptive-technology-impacting-industries>

# Business Insider (BI) Article

- AI tools could heavily impact our jobs (even replace some jobs)
- AI can automate mid-skill, mid-career tasks
- "We have to think about these things as productivity enhancing tools, as opposed to complete replacements," per Anu Madgavkar, a partner at the McKinsey Global Institute

Source: <https://www.businessinsider.com/chatgpt-jobs-at-risk-replacement-artificial-intelligence-ai-labor-trends-2023-02>

# AI Notable Quotes

- PwC: AI is set to drive global economic growth by \$15.7 trillion by 2030
- Sundar Pichai (CEO of Google): "AI is one of the most important things humanity is working on. It is more profound than, I dunno, electricity or fire."
- Andrew Ng (Co-founder of Google Brain, Coursera): "Just as electricity transformed almost everything 100 years ago, today I actually have a hard time thinking of an industry that I don't think AI will transform in the next several years."

Source: <https://www.pwc.com/us/en/services/consulting/cloud-digital/data-analytics/artificial-intelligence.html>

Source: <https://www.cnbc.com/2018/02/01/google-ceo-sundar-pichai-ai-is-more-important-than-fire-electricity.html>

Source: <https://www.gsb.stanford.edu/insights/andrew-ng-why-ai-new-electricity>

# Explosive Growth

- ChatGPT gained 1 million users in 5 days.
- In comparison, the time it took other apps to reach 1 million users:
  - Netflix – 3.5 years
  - Airbnb – 2.5 years
  - Facebook – 10 months
  - Spotify – 5 months
  - Instagram – 2.5 months
  - iPhone – 74 days
  - Threads – 30 million in 1 day

Source: <https://www.diplomacy.edu/blog/generative-AI-models-a-fun-game-that-can-easily-get-out-of-hand>

Source: <https://www.threads.net/@zuck/post/CuXCjGVrd6R?igshid=MTc4MmM1Yml2Ng%3D%3D>

# AI Technology

## Artificial Intelligence:

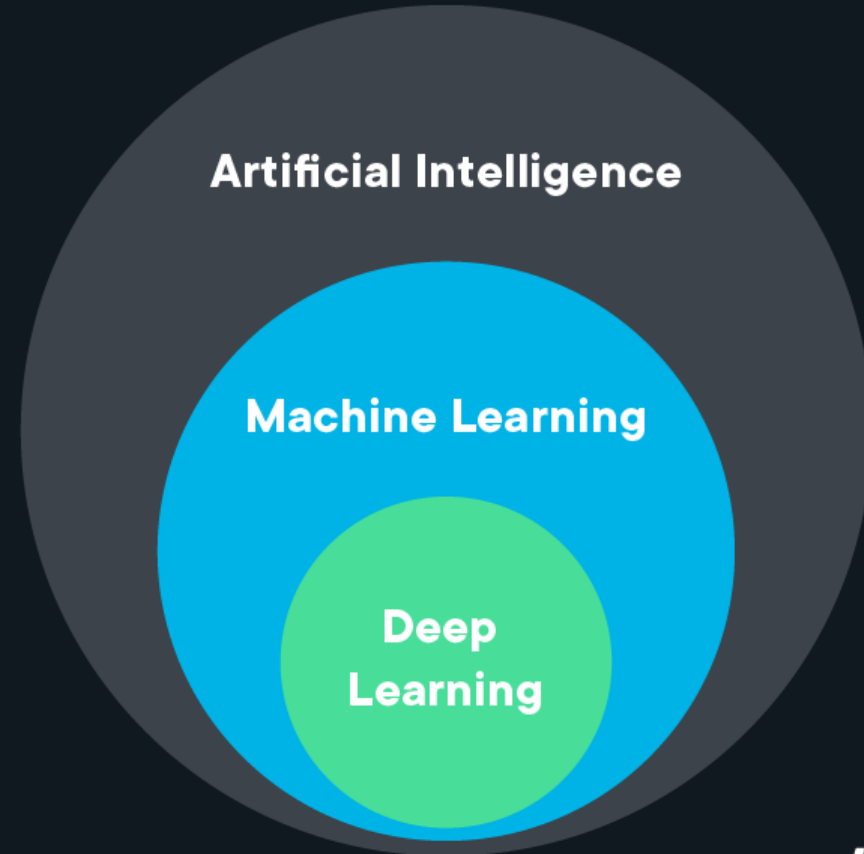
A science focused on training machines to think and act like human.

## Machine Learning:

Trains computers to perform tasks without explicit programming.

## Deep Learning:

A subset of machine learning using artificial neural networks.



# What is AI?

- At the most basic level, Artificial Intelligence (AI) uses algorithms to analyze and compare data.
- Comparison and prediction are fundamental concepts in AI.
- Through extensive datasets, AI algorithms discern patterns, enabling them to predict and make data-driven decisions.
- A goal with AI is to create machines that can learn, adapt, and potentially surpass human capabilities in performing various tasks.

# Machine Learning

- Machine learning uses algorithms and statistical models to analyze data, identify patterns, and improve performance on specific tasks without explicit programming.
- AI training is a mathematical process that involves adjusting millions or billions of parameters. AI algorithms analyze data to estimate the probability of correct predictions or classifications.
- Example: Distinguishing between images of “Cat” or “No Cat”
- Example: Machine learning can be used to predict the probability of different words that could follow an incomplete sentence. For example:
  - “I am...”
    - Happy – 5% probability
    - Sad – 3% probability

# Artificial Neural Networks

- Artificial Neural Networks (ANLs) – mimic brain functionality in machine learning.
- ANLs use virtual neurons, like brain neurons.
- In ANLs, layers process and pass information. Data represents features, like pixels or words.
- Trained ANLs – make predictions on new data by recognizing patterns from the training data, like classifying images as cats or dogs.


# Natural Language Processing (NLP)

- NLP – algorithms and techniques that can analyze, process, and generate natural language data.
- NLP – employs machine learning, deep learning, and statistical methods, to analyze human language data.
- Supervised NLP – AI learns from input-output pairs (e.g., picture-"cat" or picture-"no cat").
- ChatGPT is a self-trained NLP model that initially underwent supervised training, but now utilizes billions of parameters for its learning.

# ChatGPT

## What would you ask ChatGPT?


ES ChatGPT, what are the requirement numbers in PCI DSS v3.2.1 that require strong encryption?

 In PCI DSS v3.2.1, there are multiple requirements that emphasize the use of strong encryption to protect cardholder data. Here are some key requirements related to encryption:

1. Requirement 3: Protect stored cardholder data
  - Requirement 3.4: Render PAN (Primary Account Number) unreadable anywhere it is stored (e.g., using strong encryption or truncation).
2. Requirement 4: Encrypt transmission of cardholder data across open, public networks
  - Requirement 4.1: Use strong cryptography and security protocols (e.g., TLS/SSL) to safeguard sensitive cardholder data during transmission over public networks.
3. Requirement 4: Encrypt transmission of cardholder data across open, public networks
  - Requirement 4.2: Ensure that all encryption keys are stored securely and protected against unauthorized access.
4. Requirement 8: Identify and authenticate access to system components
  - Requirement 8.2.1: Use strong cryptography and security protocols (e.g., TLS/SSL) when transmitting login credentials.

These are just a few examples of the requirements in PCI DSS v3.2.1 that emphasize the use of strong encryption. It is important to refer to the full PCI DSS documentation for a comprehensive understanding of the encryption requirements and their specific implementation guidelines.

ES ChatGPT, what are the requirement numbers in PCI DSS v4.0 that require strong encryption?

 I apologize for any confusion, but as an AI language model, my responses are based on a mixture of licensed data, data created by human trainers, and publicly available data. I have not been directly trained on specific PCI DSS documents, such as version 4.0. Therefore, I do not have real-time access to the specific requirement numbers in PCI DSS v4.0 that pertain to strong encryption.

To obtain accurate and up-to-date information on the specific requirement numbers related to strong encryption in PCI DSS v4.0, I recommend referring to the official PCI Security Standards Council website, where you can access the official documentation and the latest version of the PCI DSS standard. This will provide you with the most reliable and current information for your PCI DSS compliance efforts.

# ChatGPT

What would you ask ChatGPT?

ES Is DES strong encryption?



The Data Encryption Standard (DES) was once considered a strong encryption standard, but by today's standards, it is no longer deemed secure against well-equipped attackers. Here's a brief overview:

1. **History and Adoption:** DES was adopted as a federal standard in the U.S. in 1977. For a long time, it was one of the most widely used symmetric encryption algorithms.
2. **Key Length:** DES uses a 56-bit key, which means there are  $2^{56}$  (or about 72 quadrillion) possible keys. While that sounds like a large number, advancements in computer hardware and specialized machinery made it feasible to attempt a brute-force attack, trying every possible key until the correct one is found.
3. **Brute-Force Attacks:** The first public demonstration of breaking DES through brute force came in 1998, when a machine built by the Electronic Frontier Foundation, named "Deep Crack," successfully decrypted a DES-encrypted message in 56 hours. The capability to crack DES only improved from there. By 2008, a group demonstrated that a DES key could be cracked in under a day for a cost of around \$10,000.
4. **Triple DES (3DES):** To bolster the strength of DES in light of its vulnerabilities, an enhancement called Triple DES (3DES) was introduced. 3DES involves applying DES encryption three times with either two or three unique keys, effectively increasing the key length. While 3DES is stronger than DES, it's slower and has its own vulnerabilities, although they are less severe than those of DES.
5. **AES - The New Standard:** Due to the vulnerabilities and weaknesses associated with DES and the need for a more robust encryption method, the Advanced Encryption Standard (AES) was established as a new standard in 2001. AES provides much stronger encryption with key sizes of 128, 192, and 256 bits.

In conclusion, while DES was considered strong when it was first introduced, it is now considered weak and outdated. If you're looking for strong encryption for modern applications, you should consider using AES or another contemporary encryption method.

# How Will AI Change PCI DSS Assessments

- Envisioning 2033 – My viewpoint
  - AI will have significant impact across every industry.
  - Investments in AI will change how businesses prepare for PCI DSS assessments.
  - PCI DSS Assessment Personal Assistant
    - Trains new hires effectively using data on top employees.
    - Personalized in-house and industry training for employees on cutting-edge technologies.



# How Will AI Change PCI DSS Assessments

- Private AI Cloud – My viewpoint
  - Confidentiality – Client data confidentiality at the highest priority.
  - Pre-assessment – early review of client systems, allowing clients to address security misconfigurations before the PCI DSS assessment, potentially advancing the assessment schedule by months.
  - AI Reviews (sandbox) – client system configurations in sandbox reviewed by AI pointing out anomalies and potential misconfigurations.
  - AI Reviews (live) – read-only access to a live production or production replicated environment.
  - Automation – AI reviews for 50% or more of work effort required for a typical PCI DSS assessment.
  - Added assurance – AI reviews 100% of the documentation submitted, and the assessor team further reviews and confirms any findings before disclosure.

# How Will AI Change PCI DSS Assessments

- Digital Personal Assistant (DPA) – My viewpoint
  - Client facing – guides clients with personalized assistance in preparing for the PCI DSS assessment.
  - Assessor facing – guides PCI DSS assessors and streamlines the assessment review processes.

# How PCI DSS Assessors Can Prepare for Future AI Capabilities

Five things a PCI DSS assessor should do to prepare to take advantage of future AI capabilities

## 1. Develop a solid understanding of AI

- The first step to take advantage of future AI capabilities is to develop a solid understanding of AI itself. PCI DSS assessors should start by learning the basics of AI, including the different types of AI, the key concepts and techniques used in AI, and the potential benefits and risks associated with AI. They should also stay up-to-date with the latest developments in AI, including new tools and technologies, emerging trends, and best practices.

## 2. Identify potential use cases for AI in PCI DSS Assessments

- Once PCI DSS assessors have a basic understanding of AI, they should start exploring potential use cases for AI in PCI DSS assessments. Some possible use cases for AI in PCI DSS assessments include automating repetitive tasks, improving data analysis and visualization, identifying anomalies and outliers in data, and predicting future trends and patterns. PCI DSS assessors should also consider how AI can be used to enhance their existing processes and workflows.

# How PCI DSS Assessors Can Prepare for Future AI Capabilities

Five things a PCI DSS assessor should do to prepare to take advantage of future AI capabilities

## 3. Build a strong data foundation

- One of the most important aspects of using AI in PCI DSS assessments is having a strong data foundation. PCI DSS assessors should focus on training AI tools with generated synthetic datasets that emulate the properties and behaviors of actual client data. Assessors can also use AI models that have been pre-trained on large datasets and then fine-tune them for PCI DSS-specific tasks using non-sensitive data.

## 4. Invest in AI tools and technologies

- To take advantage of future AI capabilities, PCI DSS assessors should invest in AI tools and technologies. This may include machine learning platforms, natural language processing tools, and data visualization software. PCI DSS assessors should also work with vendors and service providers to identify and evaluate new AI tools and technologies as they emerge.

# How PCI DSS Assessors Can Prepare for Future AI Capabilities

Five things a PCI DSS assessor should do to prepare to take advantage of future AI capabilities

## 5. Collaborate with other IT professionals

- Finally, PCI DSS assessors should collaborate with other IT professionals to explore and develop new AI capabilities. This may include working with data scientists, software developers, and other IT professionals to build and test new AI applications. PCI DSS assessors should also participate in industry events, conferences, and forums to stay up-to-date with the latest AI trends and innovations.

In conclusion, as AI continues to evolve and advance, it is becoming increasingly important for PCI DSS assessors to stay up-to-date with the latest technologies and techniques. By developing a solid understanding of AI, identifying potential use cases, building a strong data foundation, investing in AI tools and technologies, and collaborating with other IT professionals, PCI DSS assessors can prepare to take advantage of future AI capabilities and enhance their overall effectiveness and efficiency.

# In Conclusion

- PCI DSS assessors are empowered with AI tools.
- PCI DSS assessors can thrive using AI.
- AI tools will bring immense value to the PCI DSS assessment process for both assessors and clients.
- PCI DSS assessors will have increased job satisfaction with AI, as it reduces the burden of mundane and repetitive tasks.