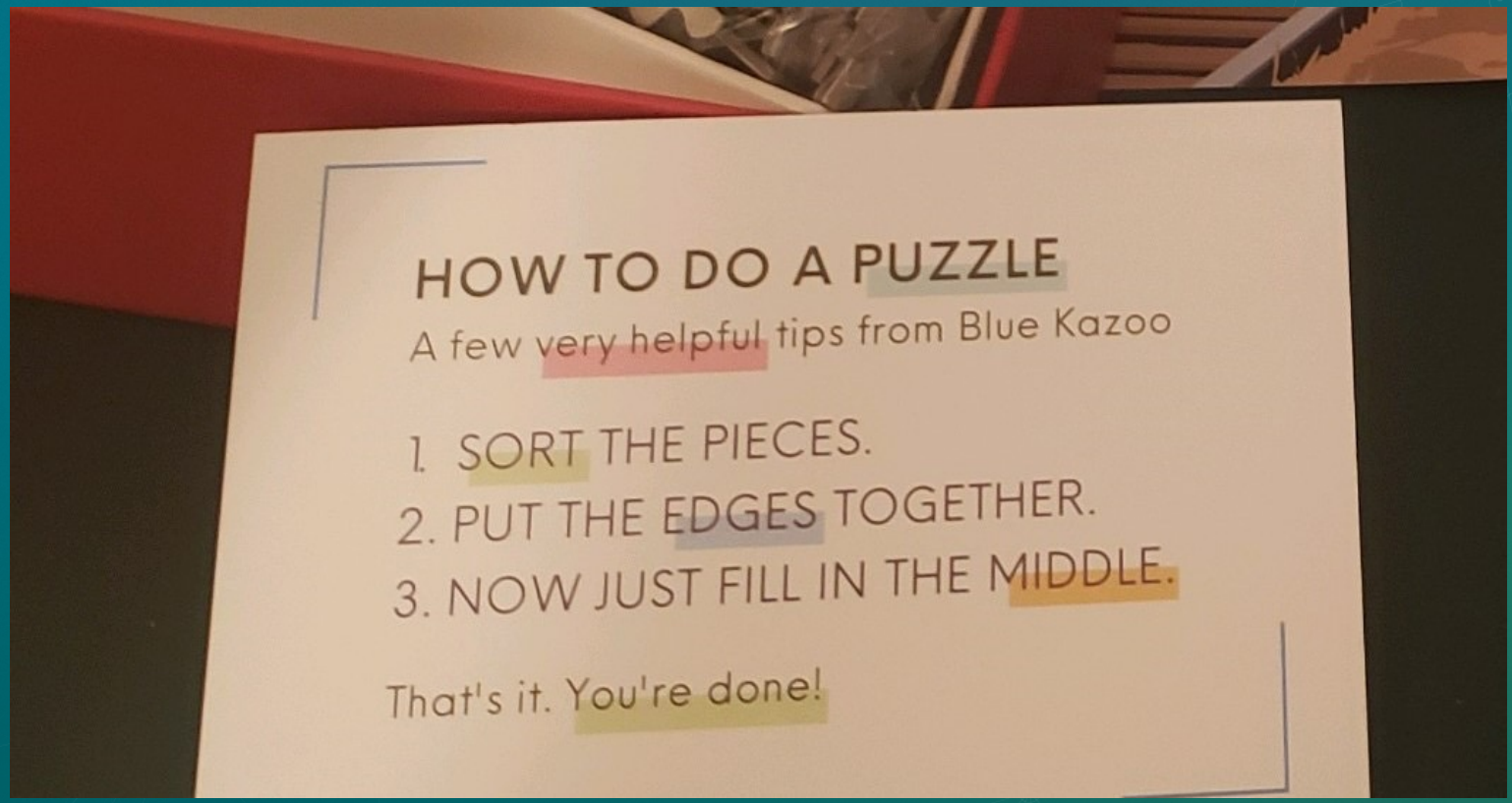
The PCI DSS Program: Take Control of the Controls

Jeni German, Digital Security Analyst
WM

The PCI DSS Program Agenda

The Program Puzzle

- **Introduction**

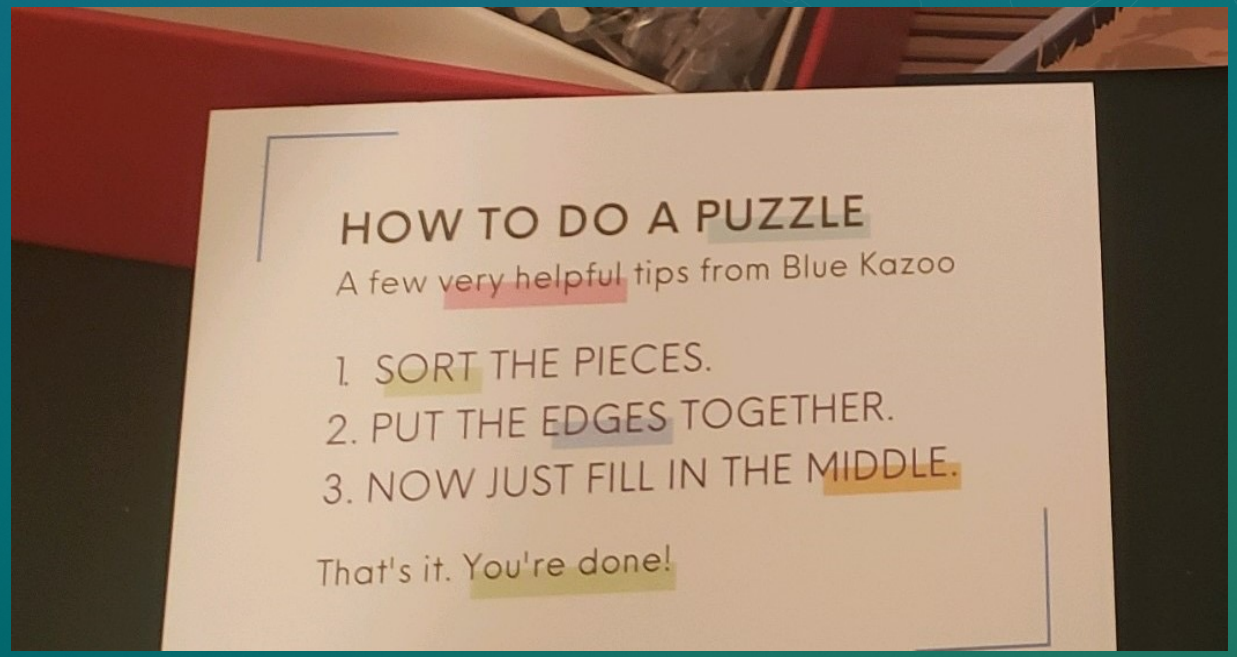


PCI Security Standards Council

The PCI DSS Program Agenda

The Program Puzzle

- **Introduction**
- **The Three Things:**
  - **Identify and Utilize the PCI DSS Program Team**

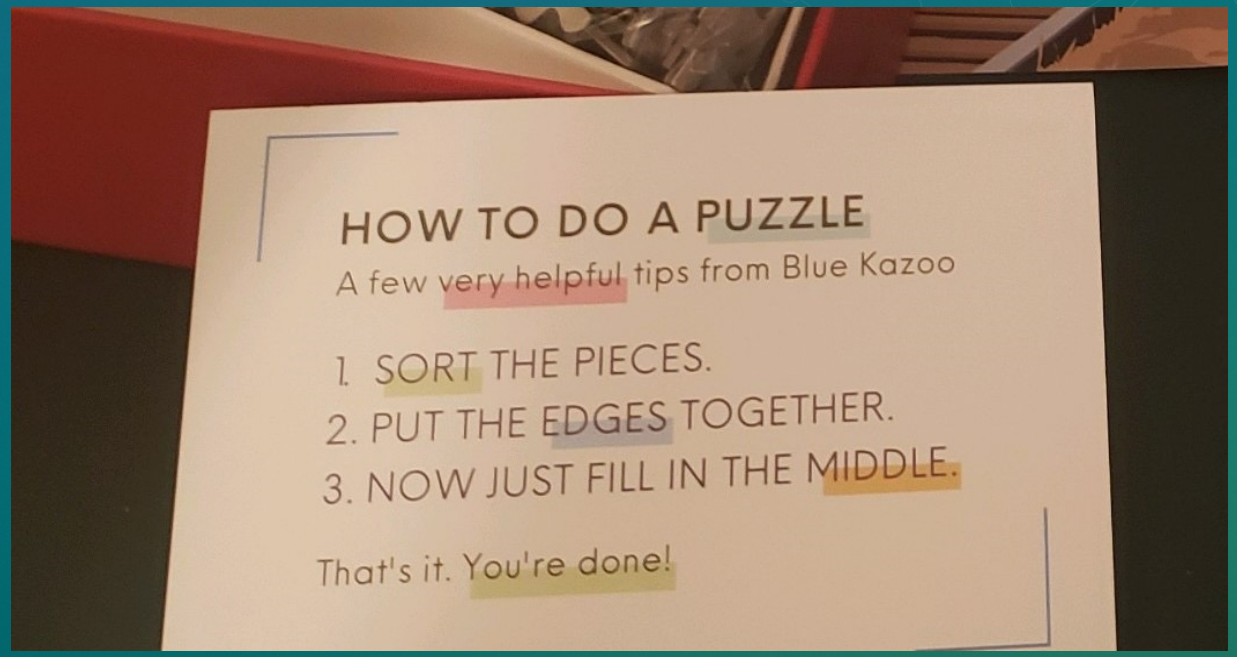


PCI Security Standards Council®

The PCI DSS Program Agenda

The Program Puzzle

- **Introduction**
- **The Three Things:**
  - **Identify and Utilize the PCI DSS Program Team**
  - **The PCI DSS Program Calendar**

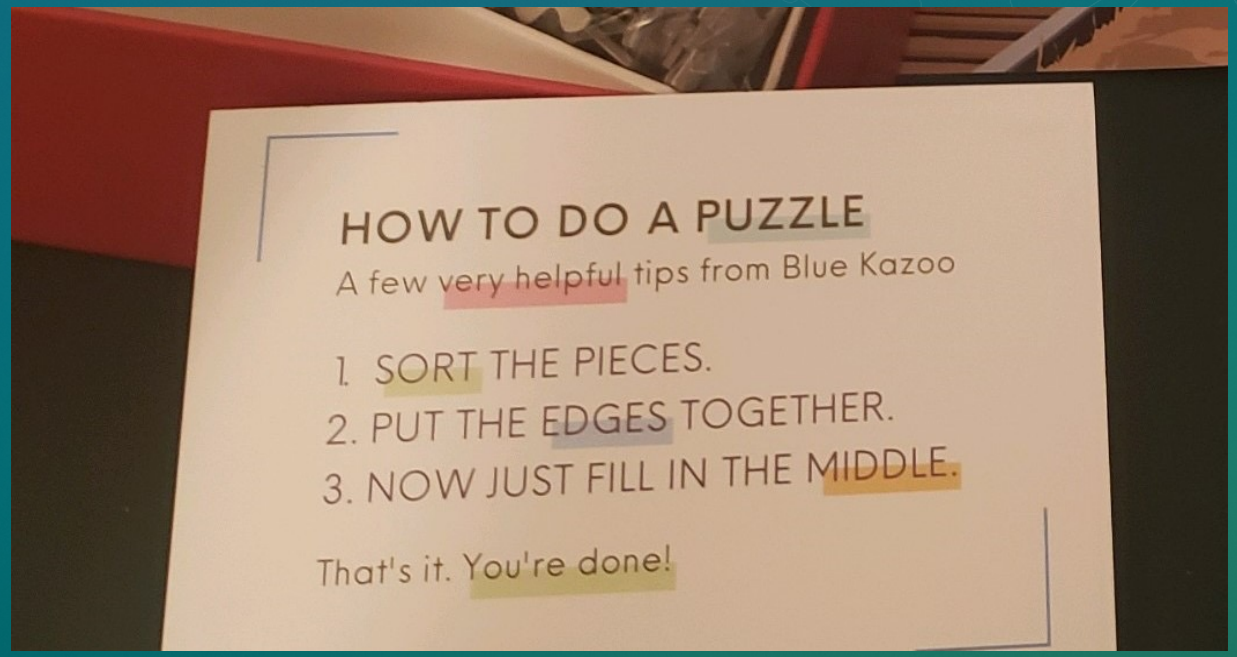


PCI Security Standards Council®

The PCI DSS Program Agenda

The Program Puzzle

- **Introduction**
- **The Three Things:**
  - **Identify and Utilize the PCI DSS Program Team**
  - **The PCI DSS Program Calendar**
  - **Streamline Evidence Collection**

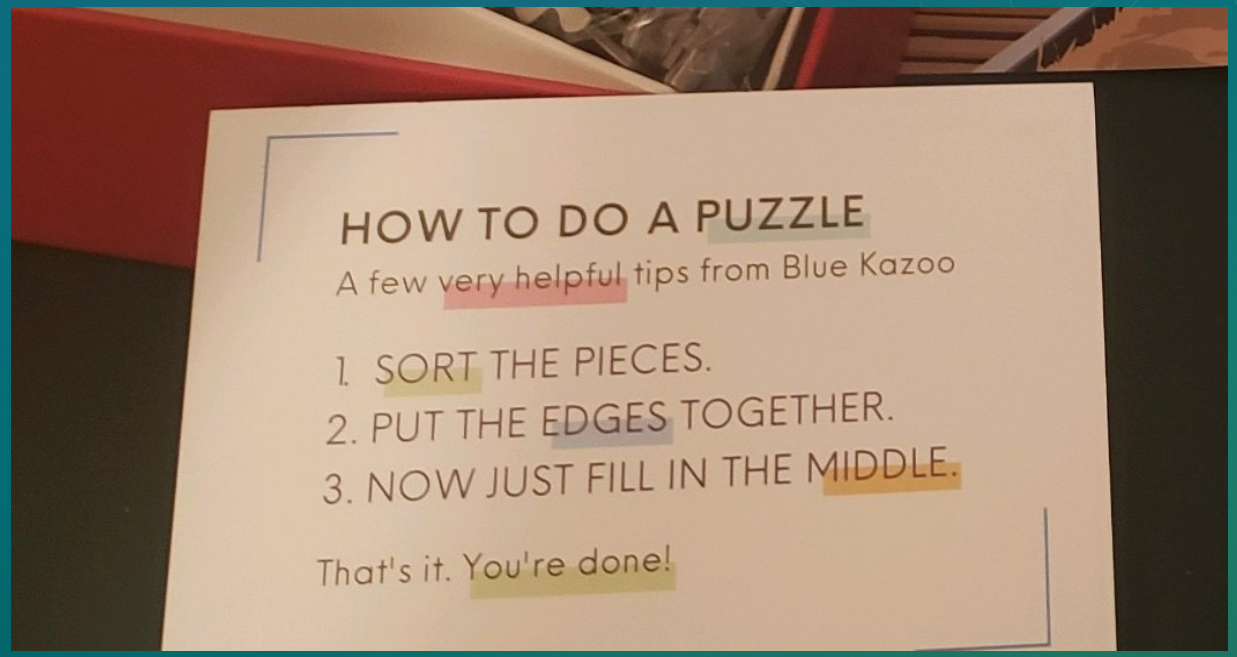


PCI Security Standards Council®

The PCI DSS Program Agenda

The Program Puzzle

- Introduction
- The Three Things:
  - Identify and Utilize the PCI DSS Program Team
  - The PCI DSS Program Calendar
  - Streamline Evidence Collection
- Take-aways



PCI Security Standards Council

The PCI DSS Program
Identify and Utilize the PCI DSS Program Team

Build Out the Edges to Define the Scope

PCI Security Standards Council

The PCI DSS Program
Identify and Utilize the PCI DSS Program Team

Build Out the Edges to Define the Scope

- **Define the scope of the Cardholder Data Environment**
  - **CDE = People, Processes and Technology**

PCI Security Standards Council®

The PCI DSS Program
Identify and Utilize the PCI DSS Program Team

Build Out the Edges to Define the Scope

- **Define the scope of the Cardholder Data Environment**
  - **CDE = People, Processes and Technology**
- **Review controls; assign control owners**

PCI Security Standards Council

The PCI DSS Program
Identify and Utilize the PCI DSS Program Team

Build Out the Edges to Define the Scope

- **Define the scope of the Cardholder Data Environment**
  - **CDE = People, Processes and Technology**
- **Review controls; assign control owners**
- **Produce scope documentation**
  - Critical Inventory
  - Network Diagrams
  - Data Flow Diagram

PCI Security Standards Council

The PCI DSS Program
Identify and Utilize the PCI DSS Program Team

Build Out the Edges to Define the Scope

- **Define the scope of the Cardholder Data Environment**
  - **CDE = People, Processes and Technology**
- **Review controls; assign control owners**
- **Produce scope documentation**
  - Critical Inventory
  - Network Diagrams
  - Data Flow Diagram
- **PCI DSS v4.0 12.5.2 – New scoping requirement**

PCI Security Standards Council

The PCI DSS Program
Identify and Utilize the PCI DSS Program Team

Build Out the Edges to Create Structure

- **Identify the PCI DSS Program Team**

PCI Security Standards Council®

The PCI DSS Program
Identify and Utilize the PCI DSS Program Team

Build Out the Edges to Create Structure

- **Identify the PCI DSS Program Team**
  - **Subject Matter Experts (SMEs)**
    - **Perform controls; can provide evidence**

PCI Security Standards Council®

The PCI DSS Program
Identify and Utilize the PCI DSS Program Team

Build Out the Edges to Create Structure

- **Identify the PCI DSS Program Team**
  - **Subject Matter experts**
    - **Perform controls; can provide evidence**
  - **Managers**
    - **Can represent multiple SMEs in a process area**
    - **Provides a path of escalation when roadblocks appear**

PCI Security Standards Council

The PCI DSS Program
Identify and Utilize the PCI DSS Program Team

Build Out the Edges to Create Structure

- **Identify the PCI DSS Program Team**
  - **Subject Matter experts**
    - **Perform controls; can provide evidence**
  - **Managers**
    - **Can represent multiple SMEs in a process area**
    - **Provides a path of escalation when roadblocks appear**
  - **Business Process Owners; Stakeholders**
    - **High-level decision makers**
    - **Relationship with banks and service providers**

PCI Security Standards Council®

The PCI DSS Program
Identify and Utilize the PCI DSS Program Team

Build Out the Edges to Create Structure

- **Using the PCI DSS Program Team**

PCI Security Standards Council

The PCI DSS Program
Identify and Utilize the PCI DSS Program Team

Build Out the Edges to Create Structure

- **Using the PCI DSS Program Team**
  - **Align the Team Members**

PCI Security Standards Council

The PCI DSS Program
Identify and Utilize the PCI DSS Program Team

Build Out the Edges to Create Structure

- **Using the PCI DSS Program Team**
  - **Align the Team Members**
  - **Keeping folks engaged resourcefully**
    - **Meetings – set up recurring**
      - **Frequent and Optional**
      - **Pre-meeting Agenda**
      - **Post-meeting Notes**

PCI Security Standards Council

The PCI DSS Program
Identify and Utilize the PCI DSS Program Team

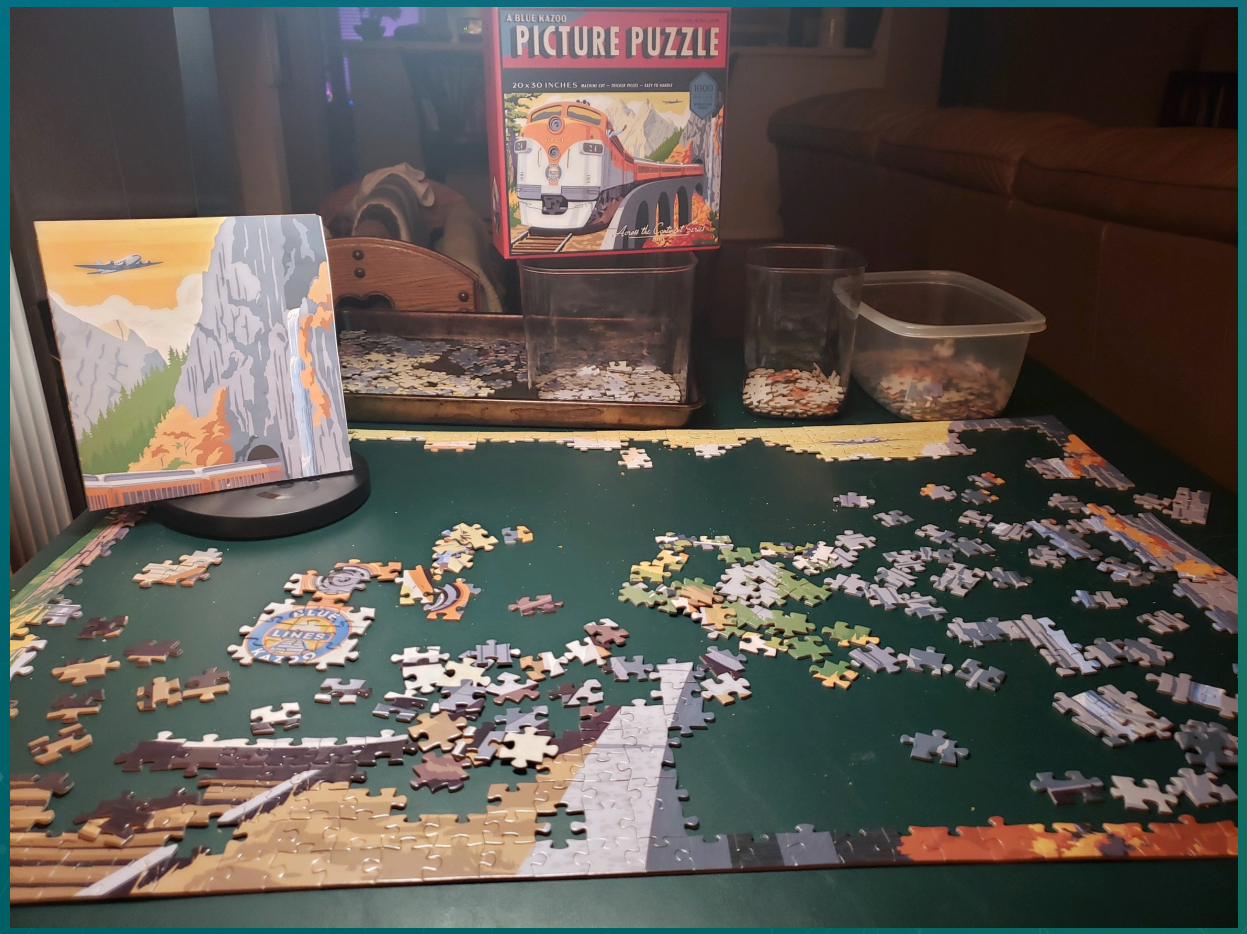
Build Out the Edges to Create Structure

- **Using the PCI DSS Program Team**
  - **Keep folks engaged resourcefully (cont'd)**
    - **Email - Copy everyone on relevant threads**
    - **Quarterly Business As Usual (BAU) calls to include the assessor**

PCI Security Standards Council

The PCI DSS Program
The Program Calendar

Fill in the Center: Planning and Workflows

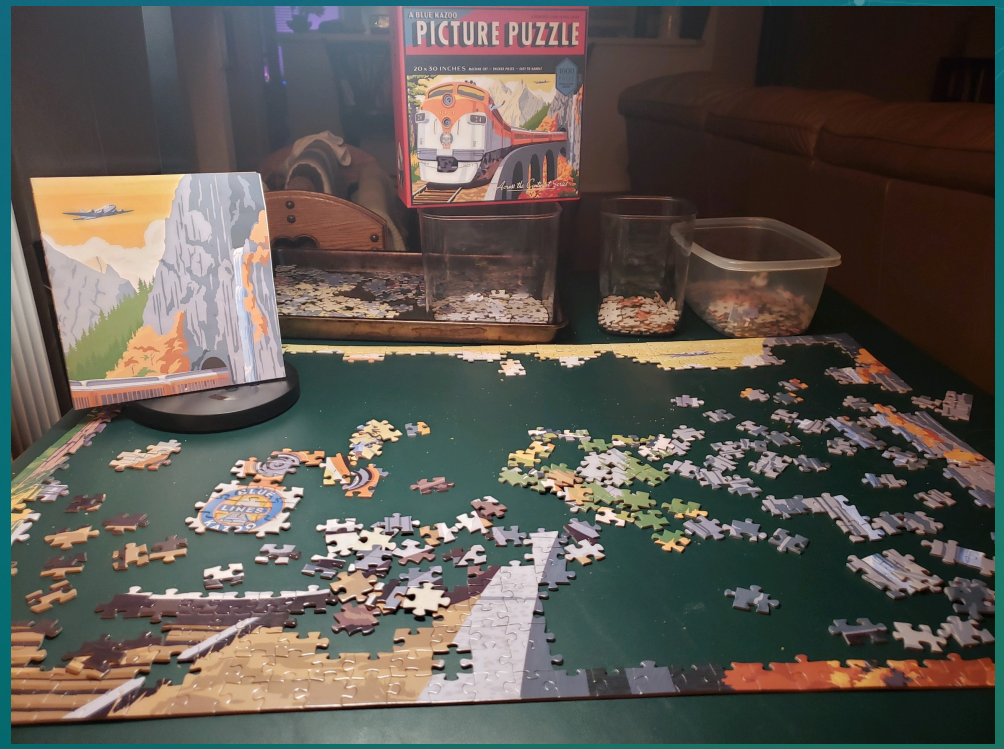


PCI Security Standards Council®

The PCI DSS Program
The Program Calendar

Fill in the Center: Planning and Workflows

- **Annual Tasks and Activities Calendar**

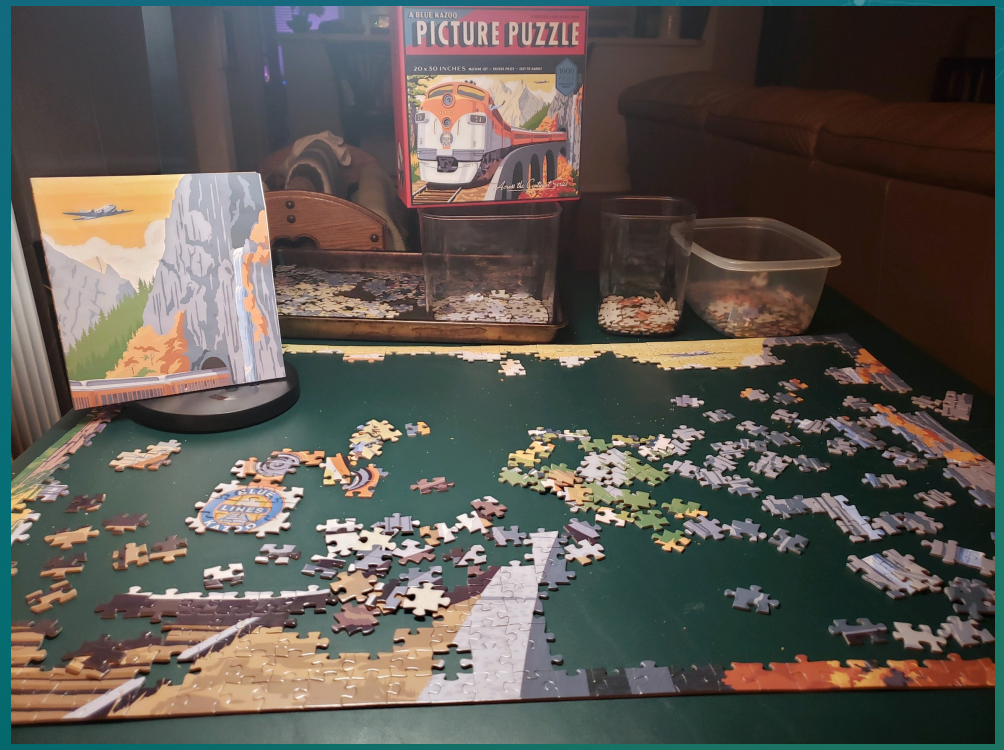


PCI Security Standards Council

The PCI DSS Program
The Program Calendar

Fill in the Center: Planning and Workflows

- **Annual Tasks and Activities Calendar**
  - **When will Program Team be in place?**
  - **Assessment Timeframe Decided**
    - **Two months within the assessment year.**
    - **Three months if using Third Party assessor**
    - **Consider business requirements and constraints**

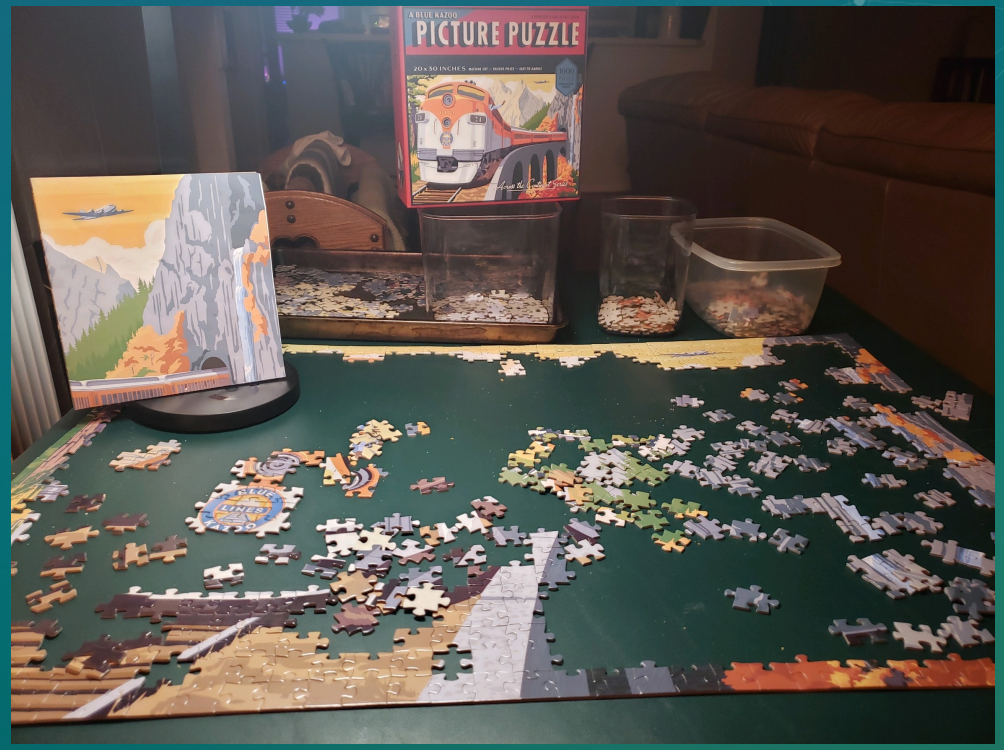


PCI Security Standards Council ®

The PCI DSS Program
The Program Calendar

Fill in the Center: Planning and Workflows

- **Annual Tasks and Activities Calendar**
  - **Scoping and documentation complete**
  - **Control Owners assigned**
  - **Dates for Evidence requests and submittal**
  - **Expected completion date**
  - **Attestation of Compliance delivery**

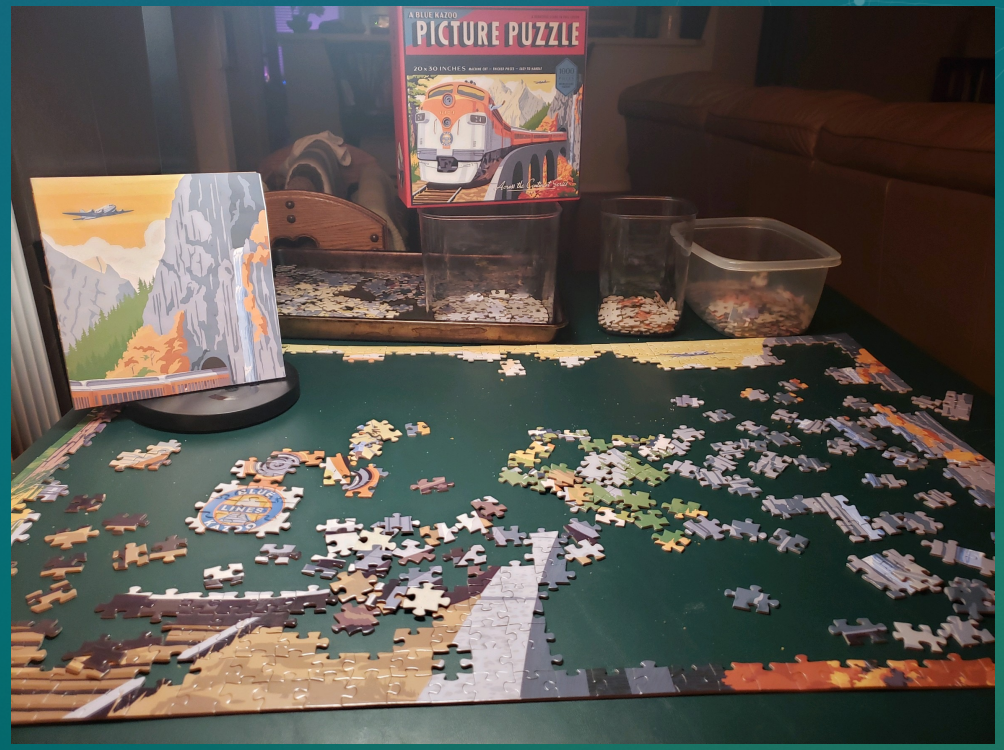


PCI Security Standards Council®

The PCI DSS Program
The Program Calendar

Fill in the Center: Planning and Workflows

- **Annual Tasks and Activities Calendar**
  - **All meetings**
    - **Program Team**
    - **BAU**
    - **Process interviews**
    - **Ad hoc activities**

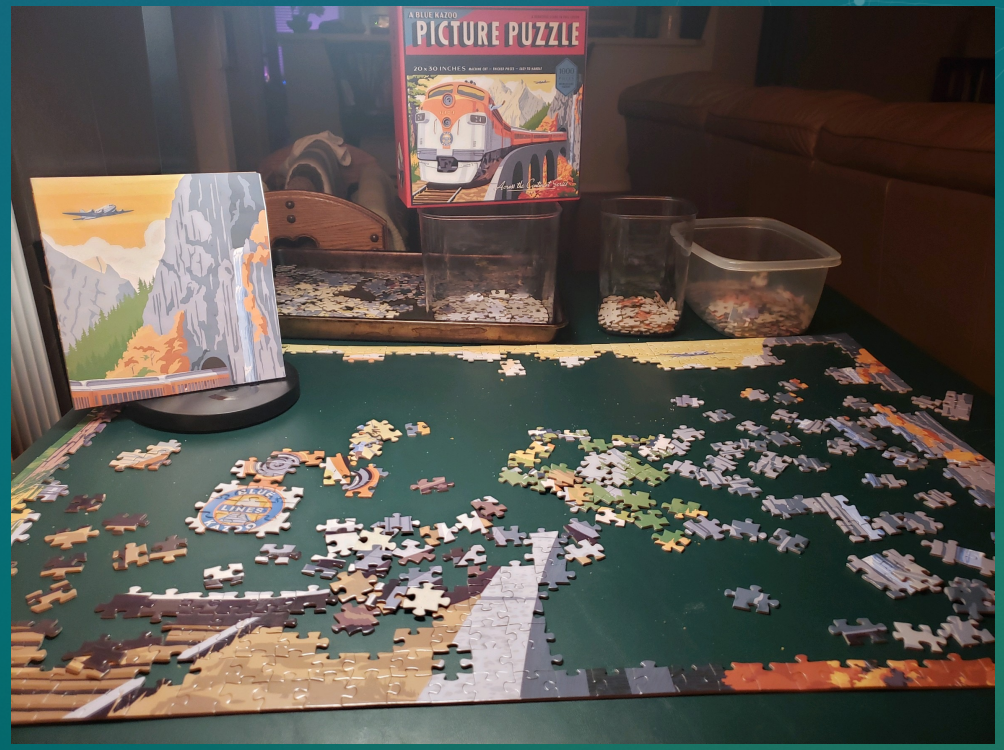


PCI Security Standards Council®

The PCI DSS Program
The Program Calendar

Fill in the Center: Planning and Workflows

- **Annual Tasks and Activities Calendar**
  - **All Annually Recurring Tasks**
    - **Time Sensitive Deliverables**
    - **ASV scans – 90 days;**
    - **Firewall Rule Reviews – six months;**
    - **Penetration Test**

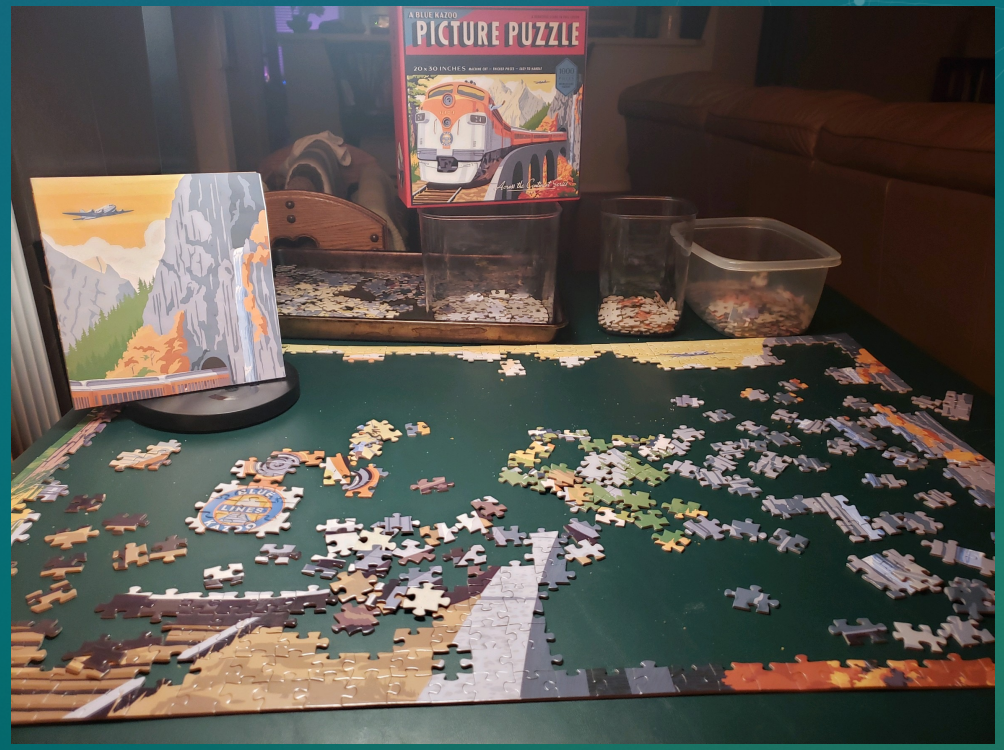


PCI Security Standards Council®

The PCI DSS Program
The Program Calendar

Fill in the Center: Planning and Workflows

- **Annual Tasks and Activities Calendar**
  - **All Annually Recurring Tasks**
    - **Time Sensitive Deliverables**
      - **ASV scans – 90 days;**
      - **Firewall Rule Reviews – six months;**
      - **Penetration Test**



Consider using the v4.0 Timeframes descriptions now!

PCI Security Standards Council

The PCI DSS Program Streamline Evidence Sources

The Picture Emerges

PCI Security Standards Council®

The PCI DSS Program Streamline Evidence Sources

The Picture Emerges

- **Look for ways to integrate processes**
  - **Policy Admin to manage policy lifecycle of all PCI DSS related policies**

PCI Security Standards Council ®

The PCI DSS Program Streamline Evidence Sources

The Picture Emerges

- Look for ways to integrate processes
  - Policy Admin to manage policy lifecycle of PCI DSS related policies
  - PCI Admin
    - To answer requests that do not need an SME.
    - Keep my eyes on things

PCI Security Standards Council

The PCI DSS Program Streamline Evidence Sources

The Picture Emerges

- Look for ways to integrate processes
  - Policy Admin to manage policy lifecycle of PCI DSS related policies
  - PCI Admin
    - To answer requests that do not need an SME
    - Keep your eye on things
- All evidence requested should come from a process in place.

PCI Security Standards Council

The PCI DSS Program Take-Aways

A Clear High Level and Detailed Picture!

PCI Security Standards Council

The PCI DSS Program Take-Aways

A Clear High Level and Detailed Picture!

1. **PCI DSS Program is not a one-person show.**

PCI Security Standards Council

The PCI DSS Program Take-Aways

A Clear High Level and Detailed Picture!

1. **PCI DSS Program is not a one-person show.**
2. **Timing is critical!**

PCI Security Standards Council®

The PCI DSS Program Take-Aways

A Clear High Level and Detailed Picture!

1. **PCI DSS Program is not a one-person show.**
2. **Timing is critical!**
3. **Functional roles might streamline evidence collection**

PCI Security Standards Council®

The PCI DSS Program Take-Aways

A Clear High Level and Detailed Picture!

1. **PCI DSS Program is not a one-person show.**
2. **Timing is critical!**
3. **Functional roles might streamline evidence collection**

Bonus Takeaway:

If a requirement cannot be answered, if a control is not in place, that could point to a gap in the security defenses. Drive the fix.

PCI Security Standards Council®