1

Active Directory Auditing for CMMC Compliance (Applied Research Associates, Inc.)

The Alexandria branch of the ARA

CHRISTOPHER KYRIACOU | DAVID FULLER | JAMIE SUTTON | NATHAN CHONG | SAFEEULLAH GHAFOORI

2

Agenda

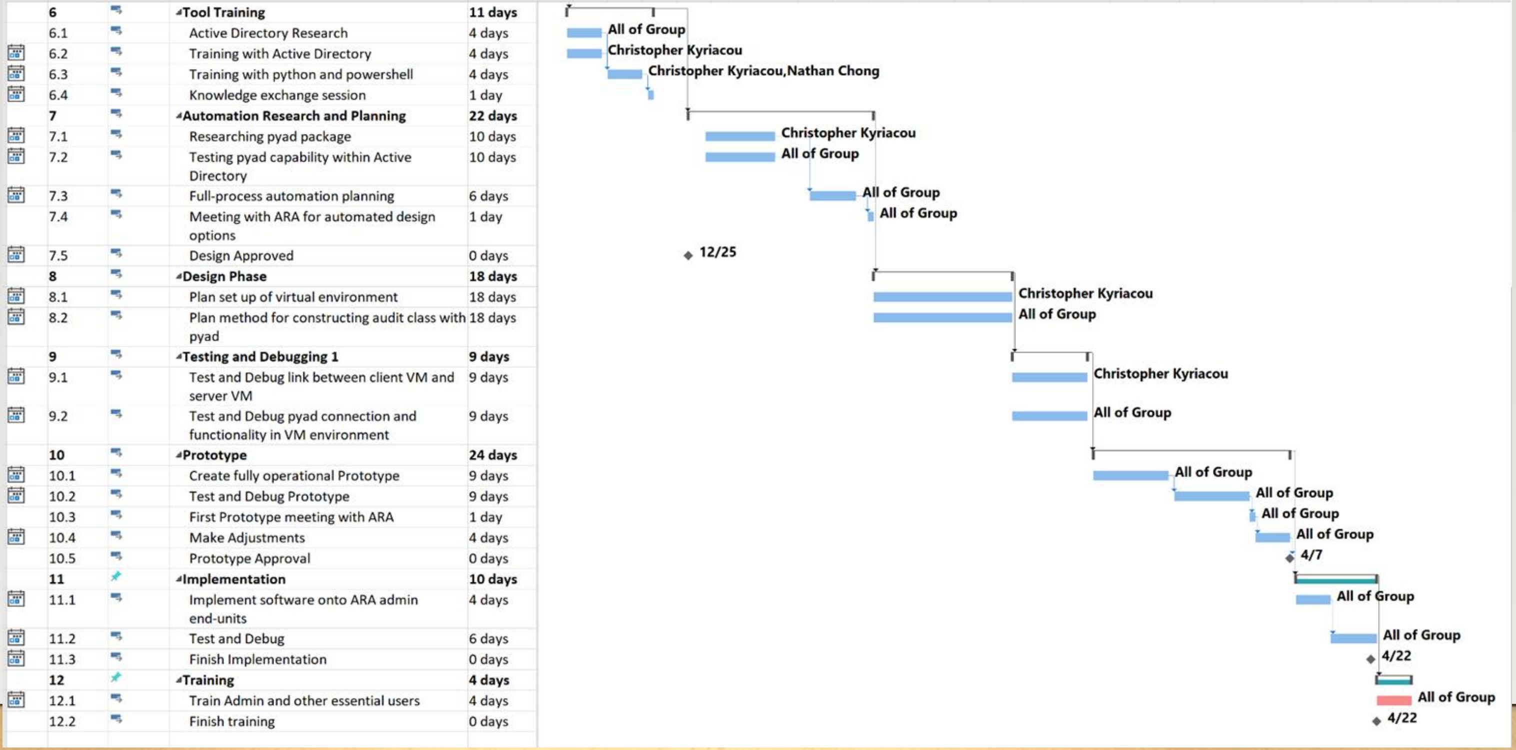
- Original Business Process
- IT Solution
- Changed Business Process
- Solutions Implementable
- Demonstration

Alpha Team 4

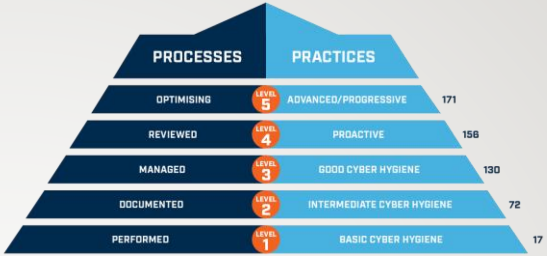
JAMIE SUTTON
SAFEEULLAH GHAFOORI
CHRIS KYRIACOU
DAVE FULLER
NATHAN CHONG

4

IT-493 Spring 2021 Project Schedule



	6	➔	**Tool Training**	**11 days**
	6.1	➔	Active Directory Research	4 days
📅	6.2	➔	Training with Active Directory	4 days
📅	6.3	➔	Training with python and powershell	4 days
📅	6.4	➔	Knowledge exchange session	1 day
	7	➔	**Automation Research and Planning**	**22 days**
📅	7.1	➔	Researching pyad package	10 days
📅	7.2	➔	Testing pyad capability within Active Directory	10 days
📅	7.3	➔	Full-process automation planning	6 days
	7.4	➔	Meeting with ARA for automated design options	1 day
📅	7.5	➔	Design Approved	0 days
	8	➔	**Design Phase**	**18 days**
📅	8.1	➔	Plan set up of virtual environment	18 days
📅	8.2	➔	Plan method for constructing audit class with pyad	18 days
	9	➔	**Testing and Debugging 1**	**9 days**
📅	9.1	➔	Test and Debug link between client VM and server VM	9 days
📅	9.2	➔	Test and Debug pyad connection and functionality in VM environment	9 days
	10	➔	**Prototype**	**24 days**
📅	10.1	➔	Create fully operational Prototype	9 days
📅	10.2	➔	Test and Debug Prototype	9 days
	10.3	➔	First Prototype meeting with ARA	1 day
📅	10.4	➔	Make Adjustments	4 days
	10.5	➔	Prototype Approval	0 days
	11	📌	**Implementation**	**10 days**
📅	11.1	➔	Implement software onto ARA admin end-units	4 days
📅	11.2	➔	Test and Debug	6 days
📅	11.3	➔	Finish Implementation	0 days
	12	📌	**Training**	**4 days**
📅	12.1	➔	Train Admin and other essential users	4 days
	12.2	➔	Finish training	0 days



PROCESSES | PRACTICES

OPTIMISING | LEVEL 5 | ADVANCED/PROGRESSIVE | 171

REVIEWED | LEVEL 4 | PROACTIVE | 156

MANAGED | LEVEL 3 | GOOD CYBER HYGIENE | 130

DOCUMENTED | LEVEL 2 | INTERMEDIATE CYBER HYGIENE | 72

PERFORMED | LEVEL 1 | BASIC CYBER HYGIENE | 17

5 CMMC Compliance

Cybersecurity Maturity Model Certification

- Primary Goal: Safeguard controlled unclassified information (CUI) across the DoD supply chain.
- CUI: Any information or data created or possessed by the government or another entity on the government's behalf.

Levels:

1. Addressing FAR 52.204-21 cybersecurity principles.
2. Build on CMMC Level 1 and addresses a little over half on NIST 800-171 controls.
3. Build on CMMC Level 2 and addresses all NIST 800-171 controls.

4 & 5. Build off CMMC Level 3 and include controls from a range of frameworks:

- CERT RMM v1.2, NIST SP 800-53, NIST SP 800-172, ISO 27002, CIS CSC 7.1, Unattributed CMMC references

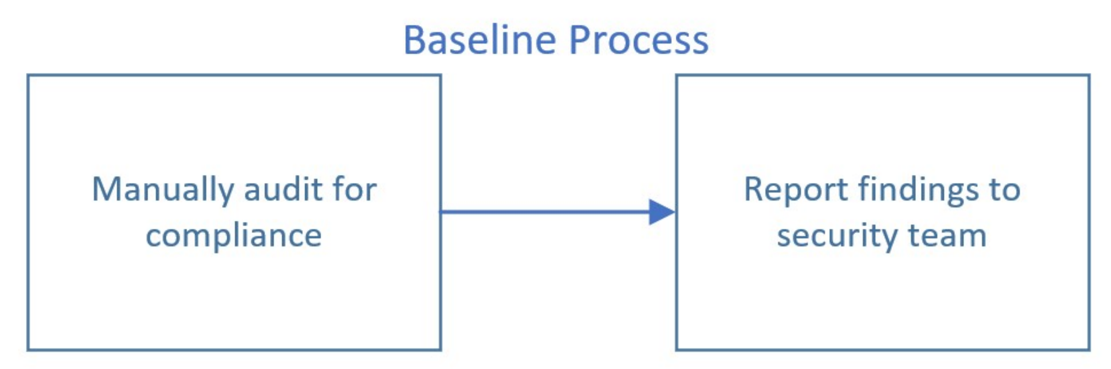
Original Business Process

6 Original Process Workflow

<u>*Quantification*</u>

- ***Auditing for:*** CMMC Level 2 Compliance
- ***Time required to conduct manual audit:*** 10 to 30 hours
- ***Frequency of audits:*** Monthly
- ***Salary for IT Admin to conduct audit:*** $83,510 per year * 2 Admins = $167,020 per year*

- **ARA Chief of Security directs admin at all 13 branches to follow this business process:**



Baseline Process

Manually audit for compliance

Report findings to security team

Original Business Process

7

Business Case for Change for Automated Auditing System

1. **Important future & current contracts will require CMMC Level 3 and up**
   a. Could be required for between 10-30% of new contracts in next 2-5 years

1. **Reduce the hours needed to audit ARA's servers across all 13 divisions**
   a. Can take days and even weeks
   b. Automated audits could be conducted daily

1. **Increase confidence in information stored within Active Directory Servers**
   a. For both ARA and Gov. Clients (DoD, DHS, etc.)

Original Business Process

8 Solution Implementation Challenges

- Fully remote contact with client
- No access to client AD servers or client network
- Implementation must be done through client and not directly
- Assumptions made about shared technical knowledge
- Communication interruptions with client
- Service Account Integration

9 *IT Solution*

Auditing Active Directory for CMMC Level 3

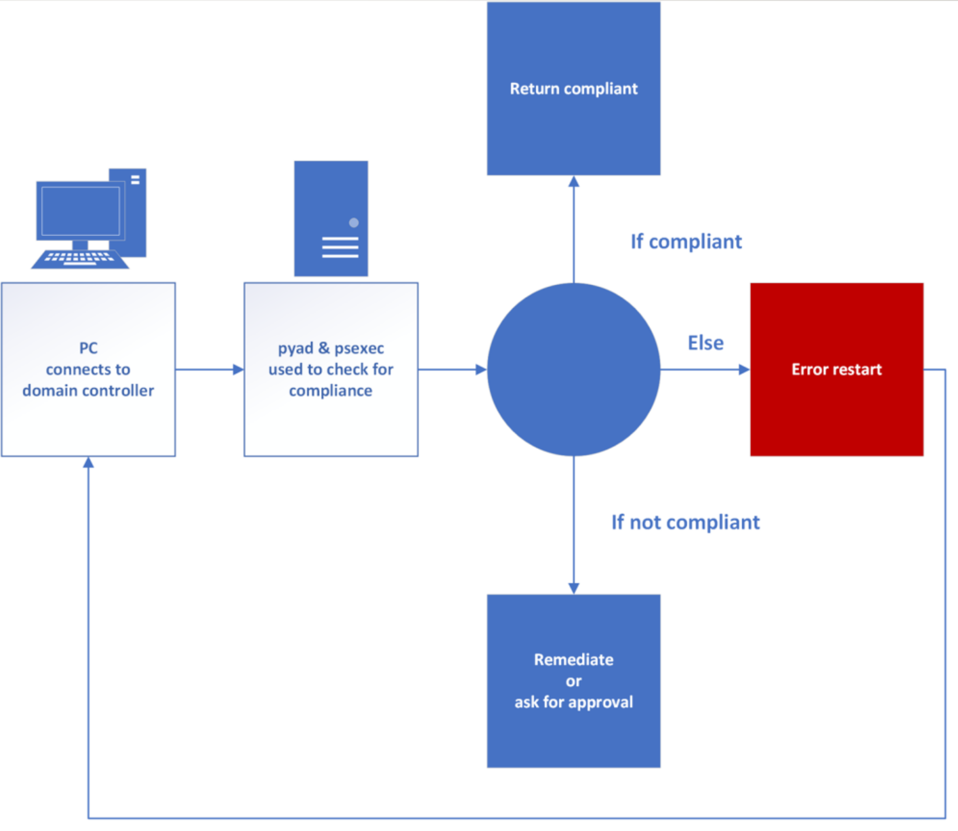
Main Objective: Create a tool that can audit AD servers to ensure **CMMC Level 3 Compliance.**

- **Must be open source and not rely on proprietary software**
- **Must be automatable (Using Ansible, etc.)**
- **Must be reliable & efficient**
- **Must be easily maintained**
- **Must be scalable & expandable (Eventually for Level 4 & 5)**
- **Must meet core functionality required by the client**

10 *IT Solution*

Desired Result

- Functions using pyad 0.6.0 & psexec to query for info
- Info passed to check if remediation is necessary
- Take appropriate action based on findings or issues that occurred
- Perform in minutes

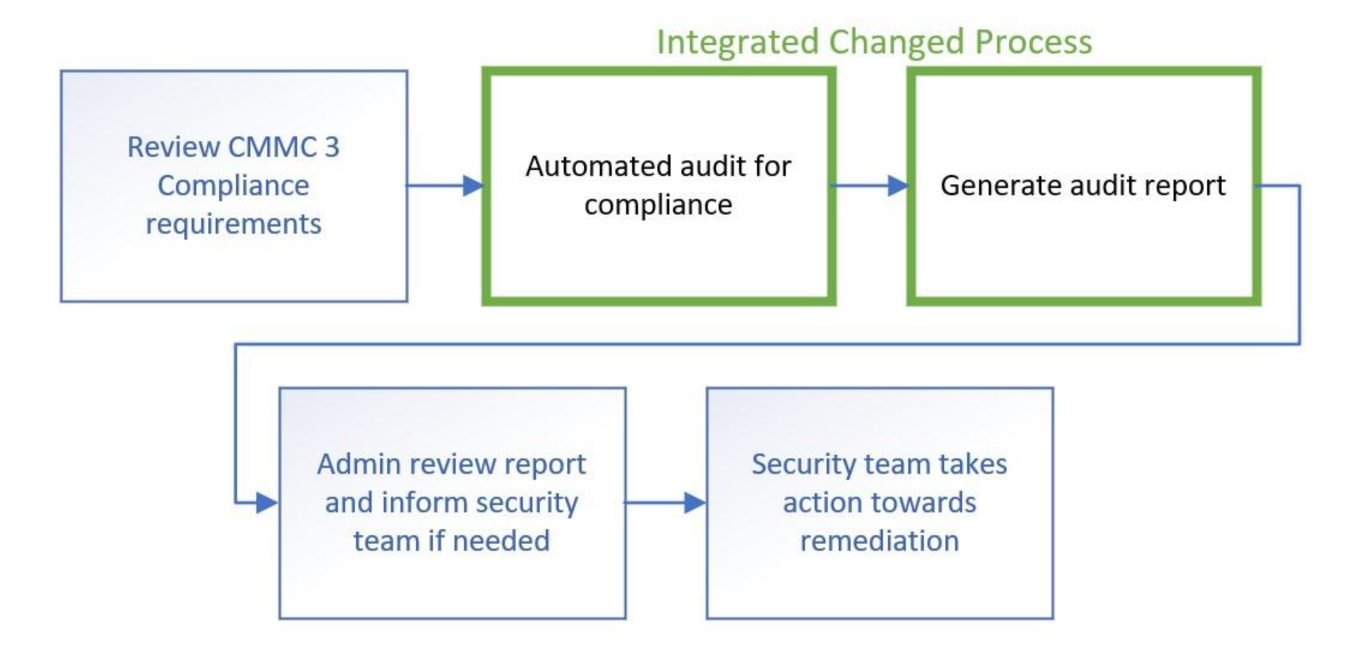


Mapping Changed Business Process to Solution Requirements

- **Changed Business Process:**
  - ○ Python scripts now automatically audit for compliance and generate audit report

- **Solution Requirements:**
  - ○ Create an auditing system that allows authorized security admin to audit their active directory servers for CMMC compliance and generate an audit report.

Overall Business Process with the Integrated Changed Process



Integrated Changed Process

Review CMMC 3 Compliance requirements

Automated audit for compliance

Generate audit report

Admin review report and inform security team if needed

Security team takes action towards remediation

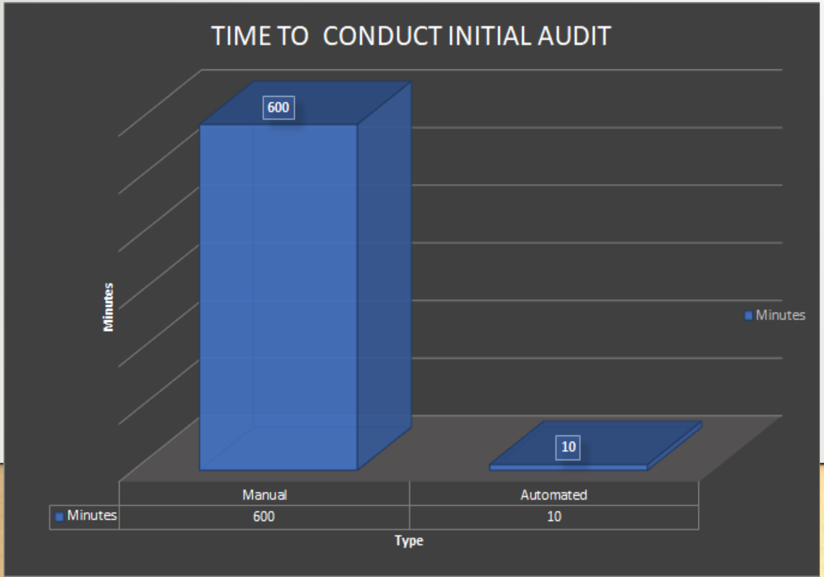
Tangible & Intangible Costs

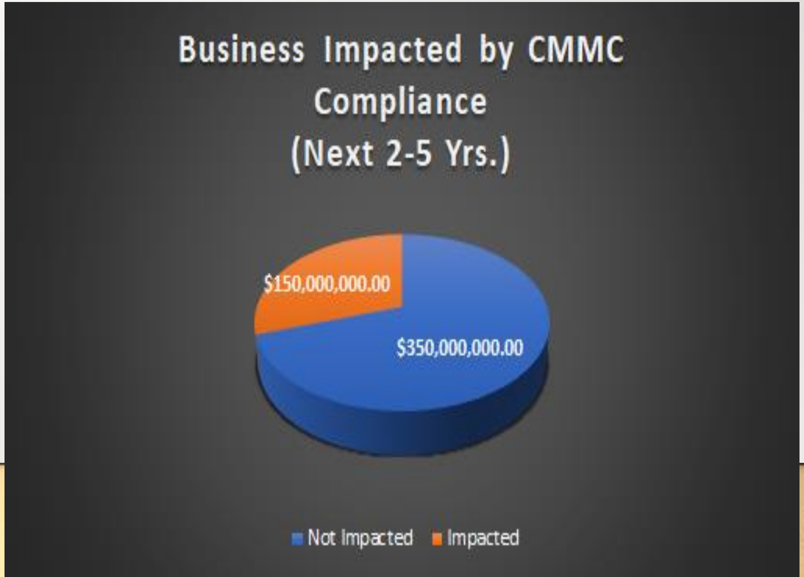
TANGIBLE COSTS:

- Labor saved: *$3,060 to $12,660/yr (Per admin)*
- Time saved: *76.5 to 316.5 hrs/yr (Per admin)*
- Implementation costs: *$0.00 (Open Source)*
- Maintenance: *Client employs proper personnel*

INTANGIBLE COSTS:

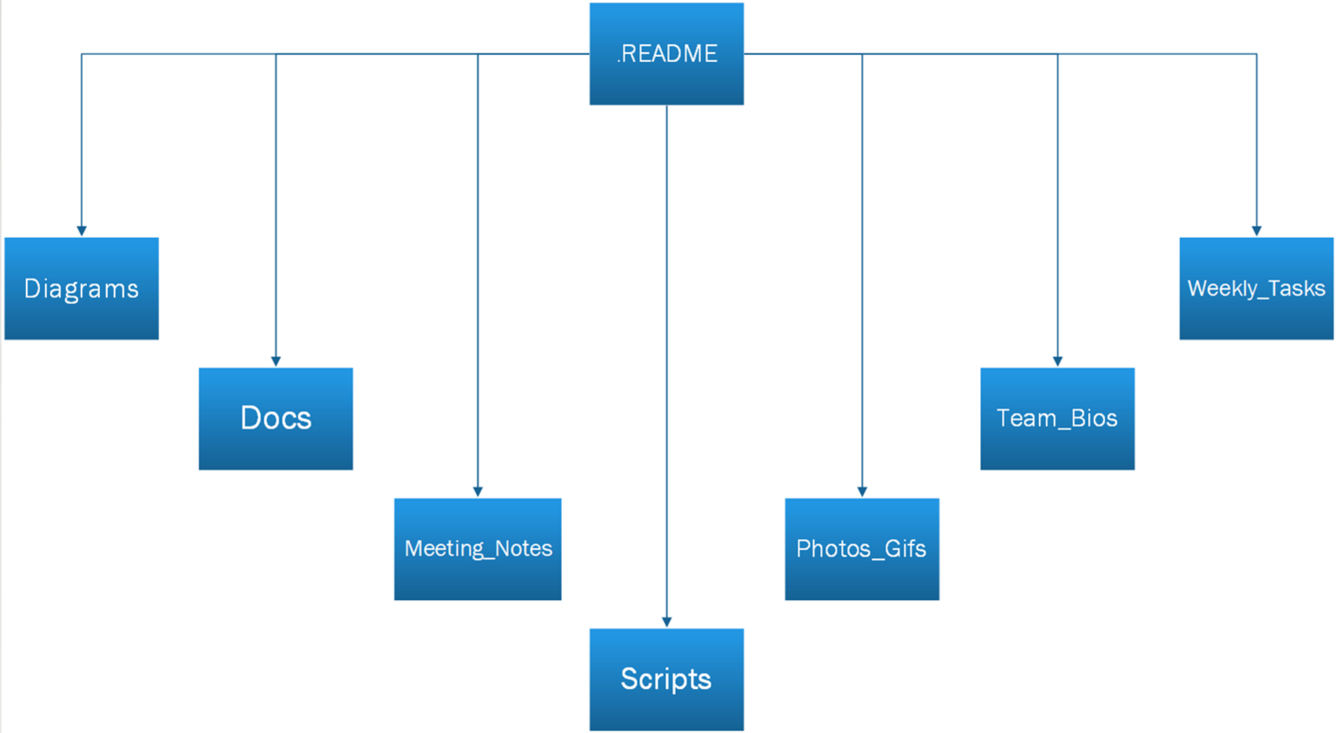
- Increase performance efficiency: *Daily audit*
- Refocus labor
- Sustain company reputation
- Achieve & sustain CMMC level 3





Solution Implementable

Documentation



Solution Implementable

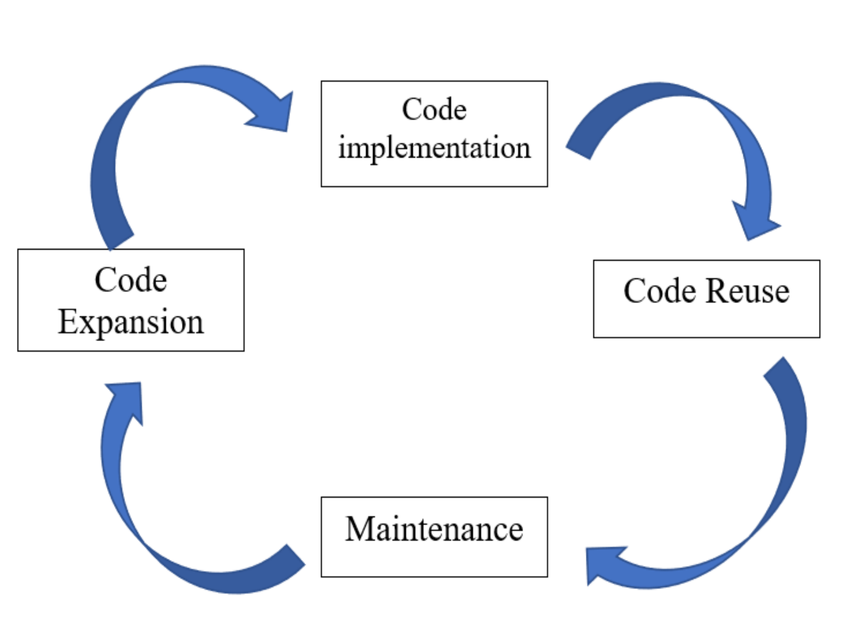
15

Solution Sustainment

- Our solution was designed with limited time in mind - meant for the ARA to implement the code in our script for reuse within their own systems

- Aiming to give the ARA the capability to expand upon what we have achieved

- Our solution is entirely open-sourced



Solution Implementable

Implementation Challenges Addressed

Challenge	Solution
- Remote contact:	- Regular meetings every 2 weeks & Github
- No access to client server(s):	- Created synonymous VM environment
- Shared knowledge constraints:	- Well documented instructions on processes
- Service Account Integration:	- Audit system can audit any service account setup

17

Solution Implementable

Project Epilogue – The Finished Product

Functional Requirement	• Satisfactory/Unsatisfactory
• Open Source?	• Satisfactory!
• Automated?	• Satisfactory!
• Easily Maintained?	• Satisfactory!
• Scaleable?	• Satisfactory!
• Address Core Functionalities?	• Satisfactory!

Demonstration

Special thanks to:

Dr. Kenneth Ingham
- Corporate Senior Security Engineer (ARA)

Thank you!

Questions?