



# ISOAG Meeting

March 1, 2017

Welcome to CESC



# Welcome and Opening Remarks

Michael Watson

March 1, 2017



# ISOAG March 1, 2017 Agenda

- |   |   |
|---|---|
| I. Welcome & Opening Remarks                      | Mike Watson, VITA   |
| II. Windows PowerShell                            | Mike Howard , Assistant Director, IS Audits US House of Representatives OIG |
| III. Risk Based Approach to Compliance Management | Karen Cole & John Brightly, Assura  |
| IV. Upcoming Events                               | Mike Watson, VITA   |
| V. Partnership Update                             | Northrop Grumman  |

# Windows PowerShell®: A Surprisingly Powerful Tool for IT Auditors and Security Professionals

---

VIRGINIA INFORMATION TECHNOLOGIES AGENCY  
INFORMATION SECURITY OFFICERS ADVISORY  
GROUP MEETING  
MARCH 1, 2017

# Agenda

- What is Windows PowerShell
- How PowerShell Can Be Used
  - Windows and Active Directory
  - Logs
  - Website and Contact Management
- How to Get Started
- Final Thoughts

“In this world,  
nothing can said to  
be certain, except  
death and taxes”

---

BEN FRANKLIN

# ... and PowerShell

---

POSSIBLY MICROSOFT

# What is PowerShell?

- Its everywhere, including now on Macs!
- PowerShell is an automation platform and scripting language for Windows and Windows Server that allows you to simplify the management of your systems. Unlike other text-based shells, PowerShell harnesses the power of the .NET Framework, providing rich objects and a massive set of built-in functionality for taking control of your Windows environments.
- Official Site:  
<https://msdn.microsoft.com/powershell>

# What is PowerShell?

- Basics of PowerShell
  - On all modern Windows operating systems beginning with Windows 7
  - An enhanced shell environment for Windows
  - Easy-to-use verb-noun syntax for commands (cmdlets)
  - Can execute non-PowerShell commands and launch programs
  - Accepts pipes “|”, allowing passing of data between commands
  - Includes a scripting language and script development program
  - Built-in help
  - Large community of PowerShell users on the Internet

# What is PowerShell?

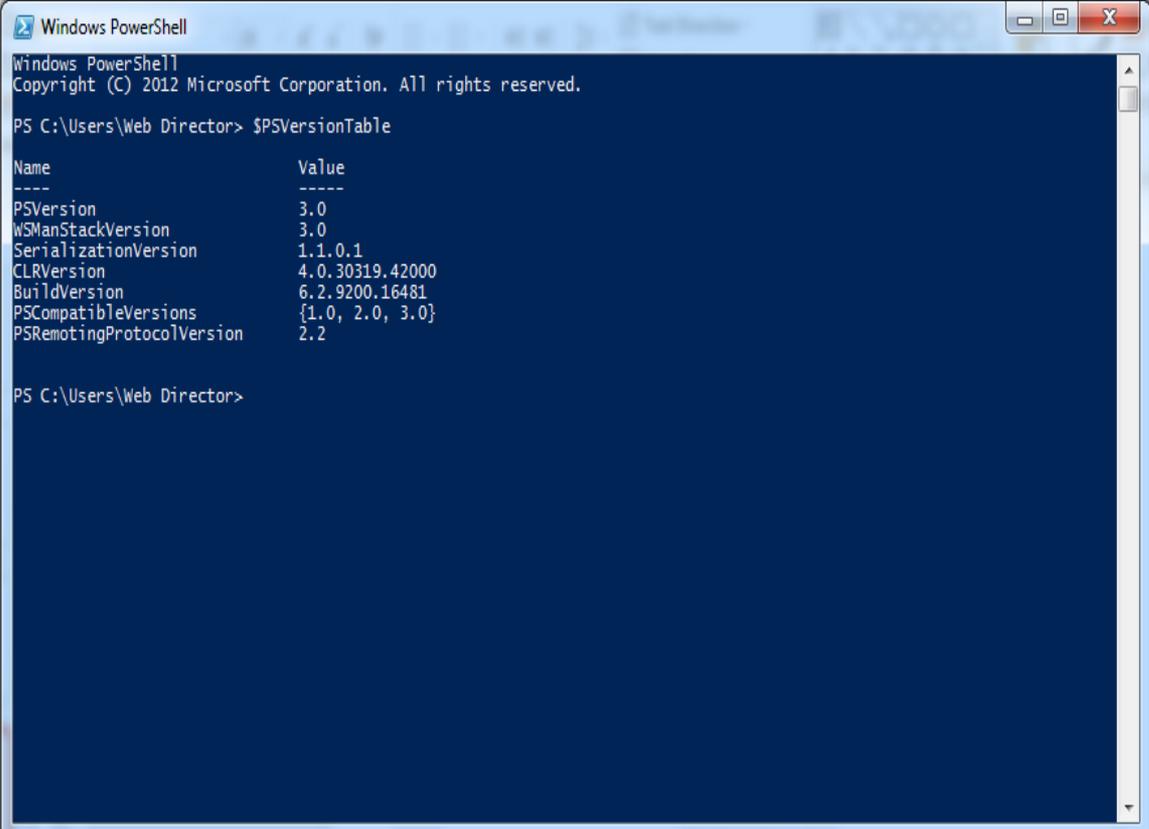
- Interfaces with Other Software
  - WMI and other Windows programs
  - Active Directory
  - Office applications (e.g. Word, Excel, Outlook)
  - SQL Server
  - SharePoint
  - Third-party software (e.g. VMware, Remedy)

# What is PowerShell?

- Data Analysis Capabilities
  - Easily imports CSV, XML, and Text Files
  - Imports Office files, including Word and Excel
  - Includes analysis commands, such as those to compare data
  - Includes editing features such as search and replace text
  - Can be used to lookup data from one file in another
  - Output can be sent to a Grid-View where data can be filtered
  - Generates output in text, CSV, and Office file formats
    - With text output, you can generate HTML files
    - Commands available to send output via e-mail

# What is PowerShell?

- Command-Line Shell



```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

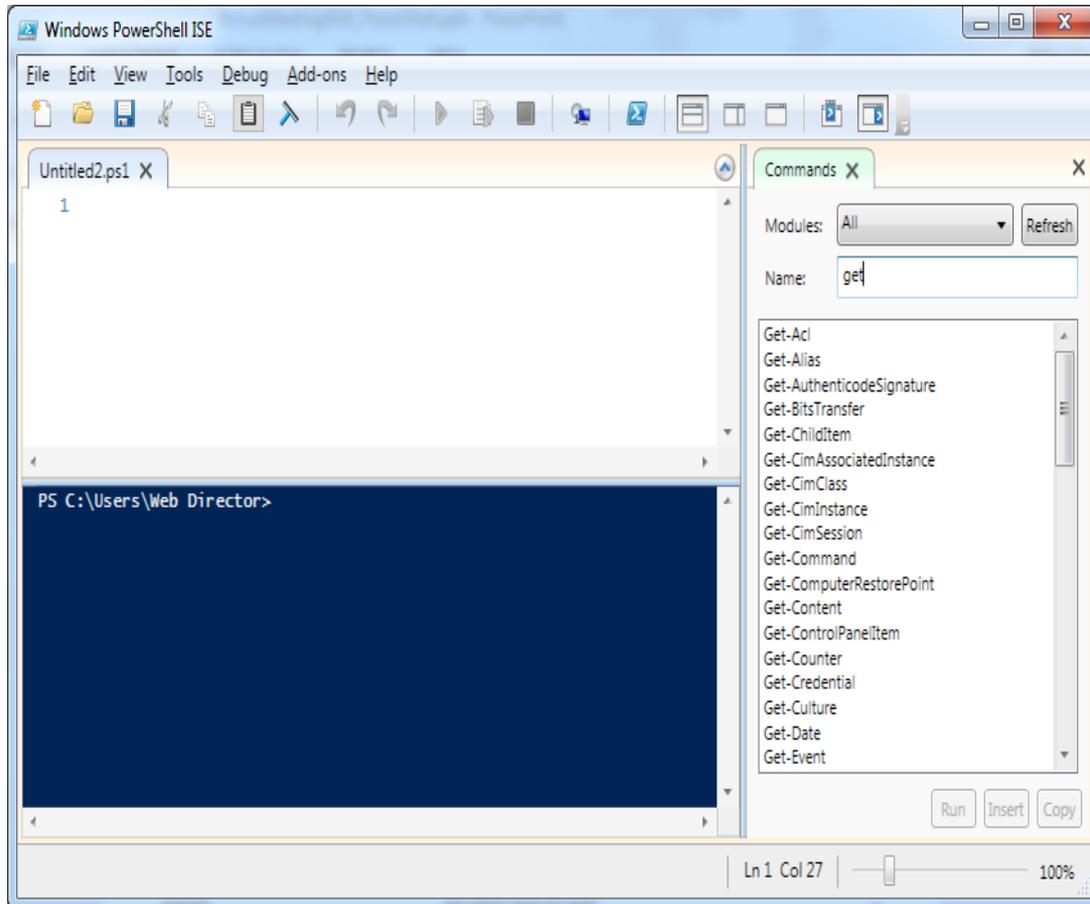
PS C:\Users\Web Director> $PSVersionTable

Name                Value
----                -
PSVersion           3.0
WSManStackVersion   3.0
SerializationVersion 1.1.0.1
CLRVersion          4.0.30319.42000
BuildVersion        6.2.9200.16481
PSCompatibleVersions {1.0, 2.0, 3.0}
PSRemotingProtocolVersion 2.2

PS C:\Users\Web Director>
```

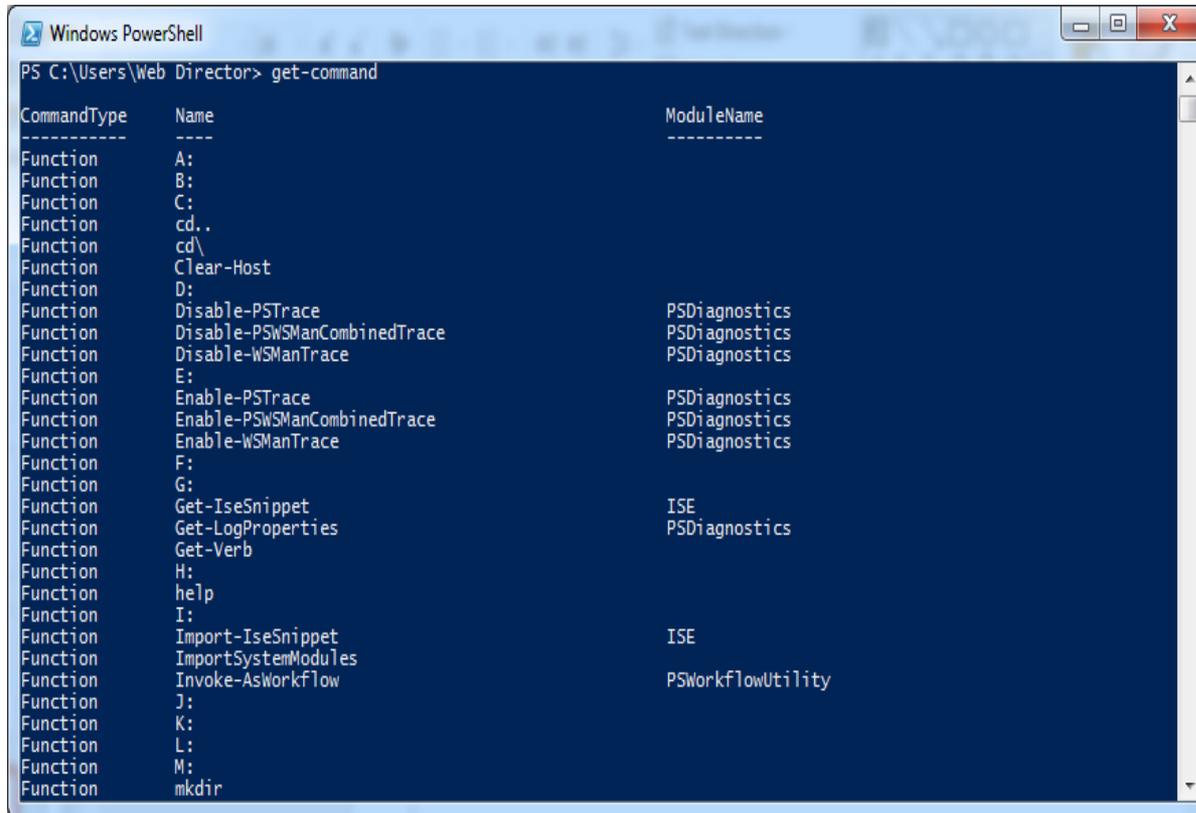
# What is PowerShell?

- Integrated Scripting Environment



# What is PowerShell?

- Built-in Directory of Commands (Cmdlets)

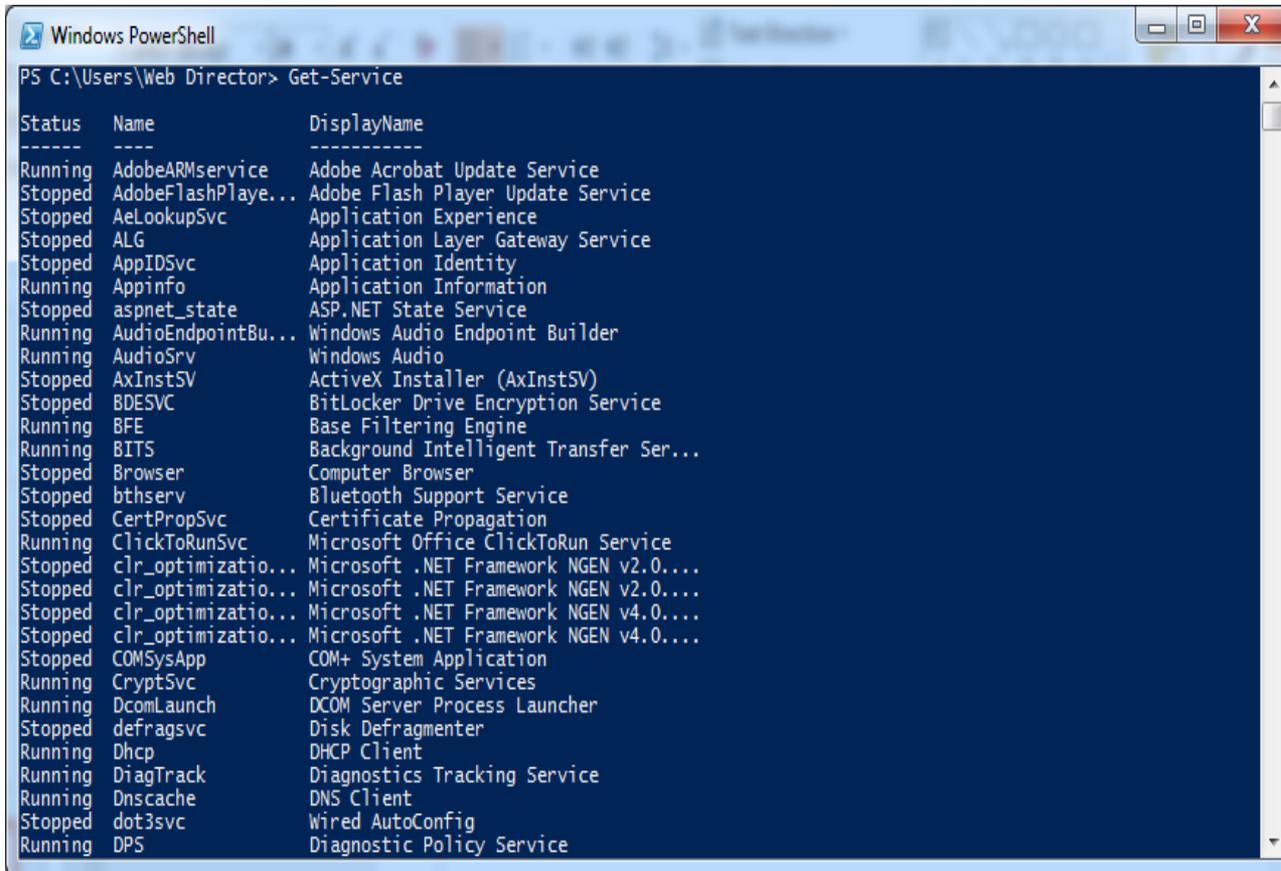


The screenshot shows a Windows PowerShell window with the title bar 'Windows PowerShell'. The command prompt shows the user is in the directory 'C:\Users\Web Director' and has entered the command 'get-command'. The output is a table listing various built-in commands (cmdlets) and their associated module names.

CommandType	Name	ModuleName
Function	A:	
Function	B:	
Function	C:	
Function	cd..	
Function	cd\	
Function	Clear-Host	
Function	D:	
Function	Disable-PSTrace	PSDiagnostics
Function	Disable-PSWSManCombinedTrace	PSDiagnostics
Function	Disable-WSManTrace	PSDiagnostics
Function	E:	
Function	Enable-PSTrace	PSDiagnostics
Function	Enable-PSWSManCombinedTrace	PSDiagnostics
Function	Enable-WSManTrace	PSDiagnostics
Function	F:	
Function	G:	
Function	Get-IseSnippet	ISE
Function	Get-LogProperties	PSDiagnostics
Function	Get-Verb	
Function	H:	
Function	help	
Function	I:	
Function	Import-IseSnippet	ISE
Function	ImportSystemModules	
Function	Invoke-AsWorkflow	PSWorkflowUtility
Function	J:	
Function	K:	
Function	L:	
Function	M:	
Function	mkdir	

# What is PowerShell?

- Verb-Noun command structure

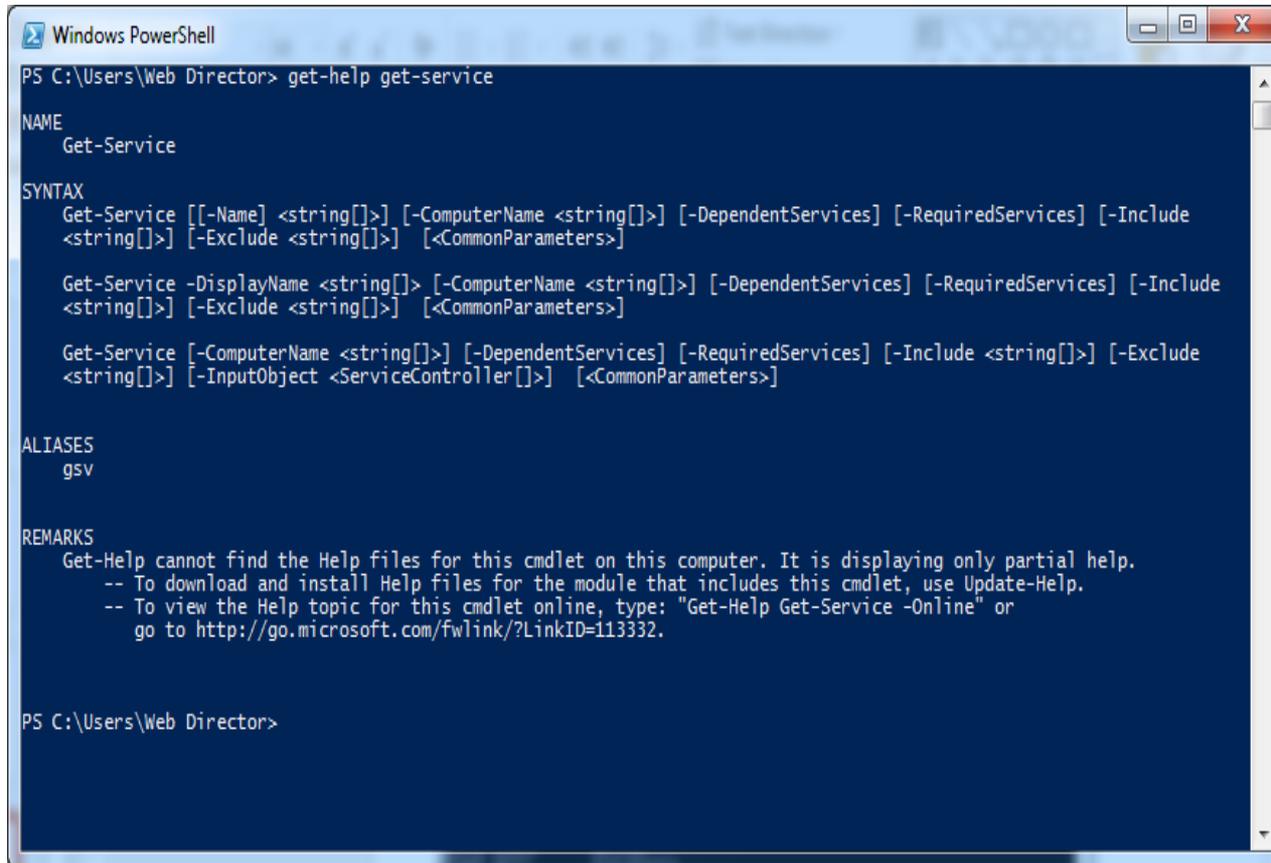


```
Windows PowerShell
PS C:\Users\Web Director> Get-Service

Status Name DisplayName
-----
Running AdobeARMService Adobe Acrobat Update Service
Stopped AdobeFlashPlaye... Adobe Flash Player Update Service
Stopped AeLookupSvc Application Experience
Stopped ALG Application Layer Gateway Service
Stopped AppIDSvc Application Identity
Running Appinfo Application Information
Stopped aspnet_state ASP.NET State Service
Running AudioEndpointBu... Windows Audio Endpoint Builder
Running AudioSrv Windows Audio
Stopped AxInstSV ActiveX Installer (AxInstSV)
Stopped BDESVC BitLocker Drive Encryption Service
Running BFE Base Filtering Engine
Running BITS Background Intelligent Transfer Ser...
Stopped Browser Computer Browser
Stopped bthserv Bluetooth Support Service
Stopped CertPropSvc Certificate Propagation
Running ClickToRunSvc Microsoft Office ClickToRun Service
Stopped clr_optimizatio... Microsoft .NET Framework NGEN v2.0...
Stopped clr_optimizatio... Microsoft .NET Framework NGEN v2.0...
Stopped clr_optimizatio... Microsoft .NET Framework NGEN v4.0...
Stopped clr_optimizatio... Microsoft .NET Framework NGEN v4.0...
Stopped COMSysApp COM+ System Application
Running CryptSvc Cryptographic Services
Running DcomLaunch DCOM Server Process Launcher
Stopped defragsvc Disk Defragmenter
Running Dhcp DHCP Client
Running DiagTrack Diagnostics Tracking Service
Running Dnscache DNS Client
Stopped dot3svc Wired AutoConfig
Running DPS Diagnostic Policy Service
```

# What is PowerShell?

- Help available on each command



```
Windows PowerShell
PS C:\Users\Web Director> get-help get-service

NAME
    Get-Service

SYNTAX
    Get-Service [[-Name] <string[]>] [-ComputerName <string[]>] [-DependentServices] [-RequiredServices] [-Include
    <string[]>] [-Exclude <string[]>] [<CommonParameters>]

    Get-Service -DisplayName <string[]> [-ComputerName <string[]>] [-DependentServices] [-RequiredServices] [-Include
    <string[]>] [-Exclude <string[]>] [<CommonParameters>]

    Get-Service [-ComputerName <string[]>] [-DependentServices] [-RequiredServices] [-Include <string[]>] [-Exclude
    <string[]>] [-InputObject <ServiceController[]>] [<CommonParameters>]

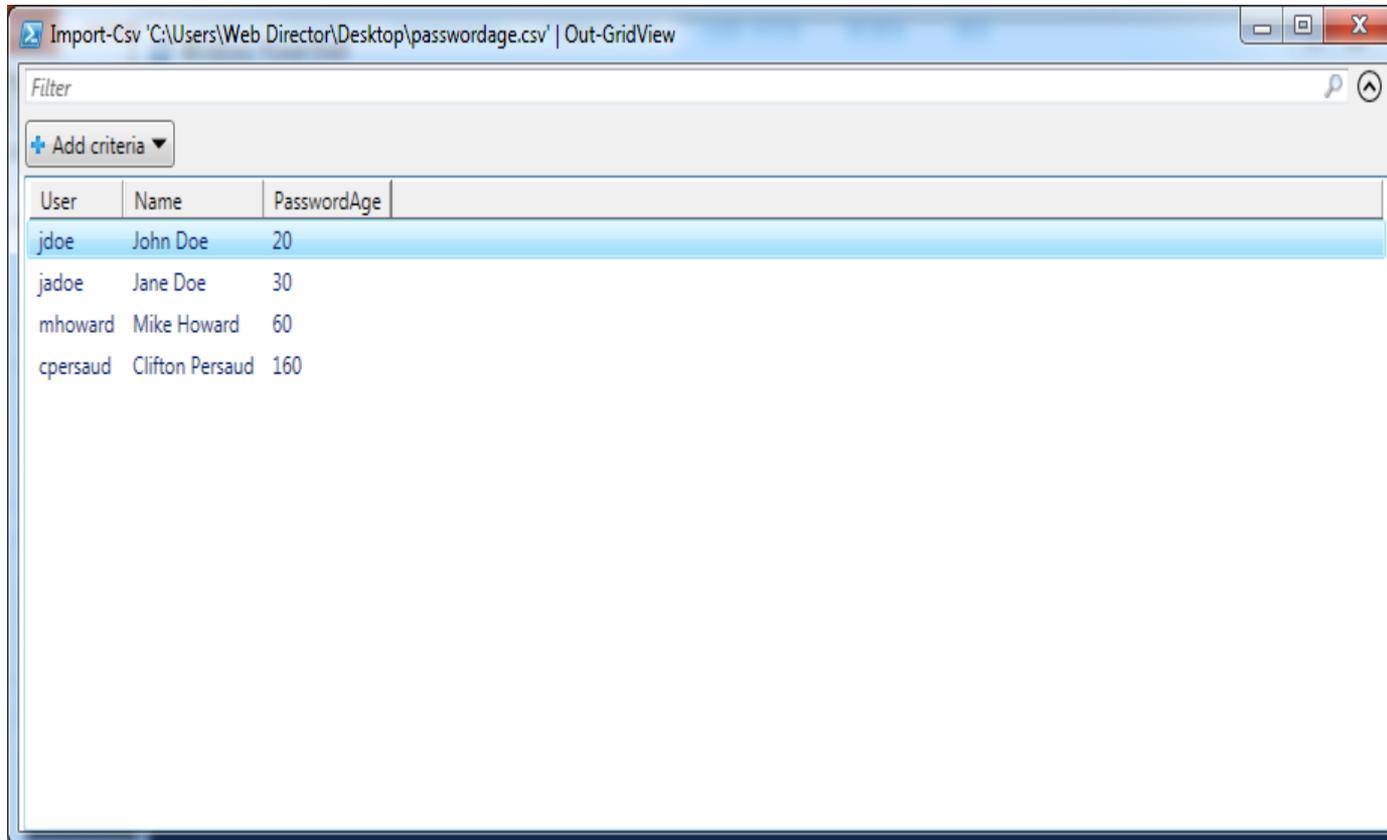
ALIASES
    gsv

REMARKS
    Get-Help cannot find the Help files for this cmdlet on this computer. It is displaying only partial help.
    -- To download and install Help files for the module that includes this cmdlet, use Update-Help.
    -- To view the Help topic for this cmdlet online, type: "Get-Help Get-Service -Online" or
    go to http://go.microsoft.com/fwlink/?LinkID=113332.

PS C:\Users\Web Director>
```

# What is PowerShell?

- Grid-View



The screenshot shows a PowerShell window titled "Import-Csv 'C:\Users\Web Director\Desktop\passwordage.csv' | Out-GridView". The window displays a table with the following data:

User	Name	PasswordAge
jdoe	John Doe	20
jadoe	Jane Doe	30
mhoward	Mike Howard	60
cpersaud	Clifton Persaud	160

“Logic will get you  
from A to B.  
Imagination will get  
you everywhere.”

---

ALBERT EINSTEIN

“In this world,  
nothing can said to  
be certain, except  
death and taxes”

---

BEN FRANKLIN

# Windows PowerShell®: A Surprisingly Powerful Tool for IT Auditors and Security Professionals

---

VIRGINIA INFORMATION TECHNOLOGIES AGENCY  
INFORMATION SECURITY OFFICERS ADVISORY GROUP  
MEETING  
MARCH 1, 2017

Imagination and  
creativity is found in  
everyone, including  
auditors and IT pros.

---

UNKNOWN AUTHOR

# How Can PowerShell Be Used?

- Uses are limited only by your imagination and the amount of time you invest in learning and using PowerShell
- It helps to have an IT problem to work on
- The tool is so robust that once you become proficient, you'll find ways to use for nearly every project, problem, or task

# How Can PowerShell Be Used?

- Perform basic Windows Functions
  - View directory and file information
  - Create directories
  - Open files and websites
  - **In practice:**
    - Created over 40 directories with common subdirectories in a matter of seconds
    - Monitor patch installation and e-mail IT administrator with recent patches

# How Can PowerShell Be Used?

- Collect Information About Windows Systems
  - View network interfaces
  - View operating system details
  - View list of running services
  - List users and groups
  - View event logs
  - View directory structure and file details
  - View directory and file permissions

# View Network Interfaces

```
Windows PowerShell
PS C:\Users\Mike> Get-WmiObject -class win32_networkadapterconfiguration | select Description, ServiceName, DHCPEnabled | ft
```

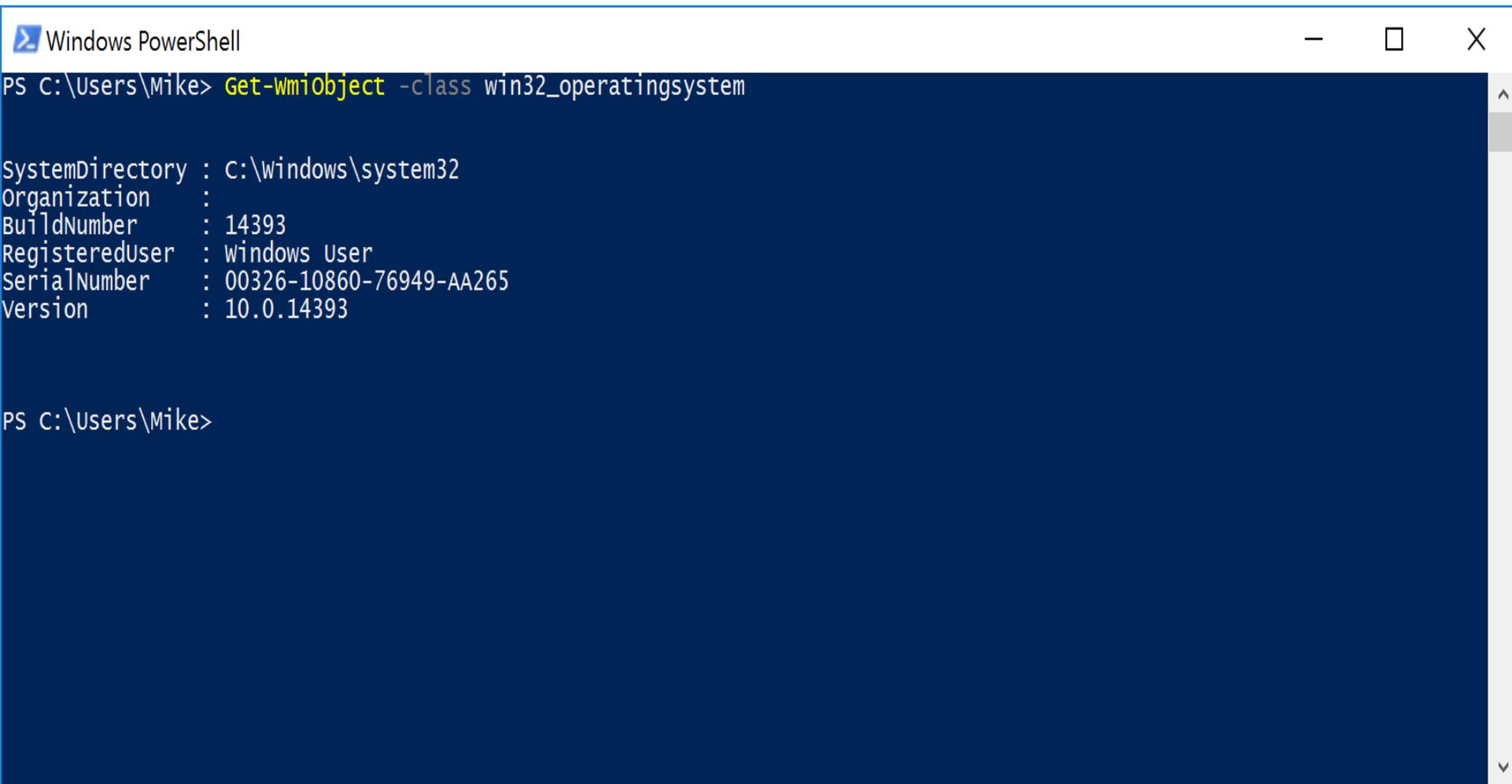
Description	ServiceName	DHCPEnabled
Microsoft Kernel Debug Network Adapter	kdnic	True
Intel(R) 82574L Gigabit Network Connection	eliexpress	True
Bluetooth Device (RFCOMM Protocol TDI)	RFCOMM	False
Bluetooth Device (Personal Area Network)	BthPan	True
Microsoft ISATAP Adapter	tunnel	False
Microsoft Teredo Tunneling Adapter	tunnel	False
Microsoft ISATAP Adapter	tunnel	False

```
PS C:\Users\Mike> Get-WmiObject -class win32_networkadapterconfiguration -filter 'IPEnabled="true"' | select Description, ServiceName, DHCPEnabled | ft
```

Description	ServiceName	DHCPEnabled
Intel(R) 82574L Gigabit Network Connection	eliexpress	True

```
PS C:\Users\Mike>
```

# View Operating System Information



```
Windows PowerShell
PS C:\Users\Mike> Get-WmiObject -class win32_operatingsystem

SystemDirectory : C:\windows\system32
Organization    :
BuildNumber     : 14393
RegisteredUser  : Windows User
SerialNumber    : 00326-10860-76949-AA265
Version         : 10.0.14393

PS C:\Users\Mike>
```

# View Running Services

```
Windows PowerShell
PS C:\Users\Mike> get-service | where-object {$_.Status -eq 'Running'} | select -first 5
```

Status	Name	DisplayName
Running	Appinfo	Application Information
Running	AudioEndpointBu...	Windows Audio Endpoint Builder
Running	Audiosrv	Windows Audio
Running	BFE	Base Filtering Engine
Running	BITS	Background Intelligent Transfer Ser...

```
PS C:\Users\Mike> get-service | where-object {$_.Status -eq 'Running'} | select * -first 5 | ft
```

Name	RequiredServices	CanPauseAndContinue	CanShutdown	CanStop	DisplayName
Appinfo	{RpcSs, ProfSvc}	False	False	True	Application Information
AudioEndpointBuilder	{}	False	False	True	Windows Audio Endpoint Bu...
Audiosrv	{AudioEndpointBuilder, RpcSs}	False	False	True	Windows Audio
BFE	{RpcSs}	False	False	True	Base Filtering Engine
BITS	{RpcSs}	False	False	True	Background Intelligent Tr...

```
PS C:\Users\Mike>
```

# View Account Information

```
Windows PowerShell
PS C:\Users\Mike> get-wmiobject -class win32_useraccount -filter 'Name="Mike"' | select AccountType, Name, Domain | ft
AccountType Name Domain
-----
512 Mike DESKTOP-6U4VG6S

PS C:\Users\Mike> net user Mike
User name           Mike
Full Name
Comment
User's comment
Country/region code 000 (System Default)
Account active       Yes
Account expires      Never

Password last set    9/8/2016 3:08:12 PM
Password expires     Never
Password changeable  9/8/2016 3:08:12 PM
Password required    No
User may change password Yes

workstations allowed All
Logon script
User profile
Home directory
```

# View Group Information

```
Windows PowerShell
PS C:\Users\Mike> get-wmiobject -class win32_group | select Name
Name
----
Administrators
Distributed COM Users
Event Log Readers
Guests
IIS_IUSRS
Performance Log Users
Performance Monitor Users
Remote Management Users
System Managed Accounts Group
Users

PS C:\Users\Mike> net localgroup Administrators
Alias name     Administrators
Comment       Administrators have complete and unrestricted access to the computer/domain

Members

-----
Administrator
Mike
The command completed successfully
```

# View Event Log Information

```
Administrator: Windows PowerShell
PS C:\windows\system32> Get-WinEvent -LogName Security | select -First 15

ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated          Id LevelDisplayName Message
-----
2/27/2017 8:23:31 PM 4799 Information A security-enabled local group membership was enumerated....
2/27/2017 8:23:21 PM 4799 Information A security-enabled local group membership was enumerated....
2/27/2017 8:22:51 PM 4799 Information A security-enabled local group membership was enumerated....
2/27/2017 8:20:38 PM 4798 Information A user's local group membership was enumerated....
2/27/2017 8:20:38 PM 4798 Information A user's local group membership was enumerated....
2/27/2017 8:20:31 PM 4798 Information A user's local group membership was enumerated....
2/27/2017 8:19:59 PM 4798 Information A user's local group membership was enumerated....
2/27/2017 8:19:59 PM 4798 Information A user's local group membership was enumerated....
2/27/2017 8:19:22 PM 4798 Information A user's local group membership was enumerated....
2/27/2017 8:18:59 PM 4798 Information A user's local group membership was enumerated....
2/27/2017 8:18:50 PM 4798 Information A user's local group membership was enumerated....
2/27/2017 8:18:33 PM 4798 Information A user's local group membership was enumerated....
2/27/2017 8:18:33 PM 4798 Information A user's local group membership was enumerated....
2/27/2017 8:18:33 PM 4798 Information A user's local group membership was enumerated....
2/27/2017 8:18:33 PM 4798 Information A user's local group membership was enumerated....

PS C:\windows\system32>
```

# How Can PowerShell Be Used?

- Audit Windows Systems against a Baseline
  - Use PowerShell to collect data from Windows system(s)
    - **Test, test, test and get client buy-in before running in production!**
  - Prepare a file of baseline settings
  - Import Windows settings and baseline into PowerShell
  - Use data analysis commands, such as compare-object, to compare settings against baseline to determine compliance
  - Multiple systems can be assessed and results output into a consolidated file
  - **In practice:** Audited over 300 Windows systems using this approach.

# How Can PowerShell Be Used?

- Review Windows Event Logs
  - Find the proverbial “needle in a haystack”
  - Windows event logs can be retrieved using PowerShell, both locally and remotely
  - PowerShell’s ability to read XML data allows for creation of a rich log data set
  - Filtering capabilities provide means for exceptions to be identified
  - Output capabilities provide options for exporting data to CSV files and web pages
  - **In practice:** Have generated daily report of log exceptions that is e-mailed daily to IT management and staff.

# How Can PowerShell Be Used?

- Audit Active Directory
  - No more sampling!
  - Query and download detailed user and computer account details, such as password age, last logon, etc.
  - Query and download group memberships
  - Query and download Group Policy Objects (GPO)
  - **In Practice:**
    - Audited user password compliance
    - Audited groups for excessive members
    - Audited GPO setting compliance
    - Obtained data for use in other audits

# How Can PowerShell Be Used?

- Audit of VMware® vCenter
  - VMware provides a plugin to PowerShell to interface with vCenter: VMware vSphere PowerCLI
  - Commands allow you to query vCenter for just about everything that can be viewed through vCenter
  - Using PowerCLI, you can audit:
    - Virtual Machine Settings
    - vCenter Access and Permissions
    - Virtual Network Configuration
  - **In practice:** Audited vCenter configuration and over 400 Virtual Machine configurations (No Sampling!)

# How Can PowerShell Be Used?

- Consolidate Data into Single Report
  - Data in a common format can be imported into PowerShell and combined into a single data set
  - PowerShell can search directories for file names with similar naming convention
  - **In Practice:**
    - Consolidated network scans of over 300 systems
    - XML data for the network scans contained more information, such as exploit information, than the standard report
    - Used Grid-View to review individual scan results for reportable weaknesses
    - Used filtering capabilities to filter out low-risk vulnerabilities

# How Can PowerShell Be Used?

- Review website logs
  - PowerShell can process all types of data, as long as its structured
  - Import and format web logs
  - Filter out Google-bots and other search engine crawlers to identify legitimate users
  - Build custom reports to track website growth
  - Generate web-friendly reports
  - **In practice:** Monitoring website logs for well over a year. Changed website links to allow metrics to be generated from the logs.

# How Can PowerShell Be Used?

- Example website log report

Membership Statistics Report x Communications Report for A... x +

file:///C:/Users/Web Director/Desktop/WebSit

Overall Metrics

The following metrics are used to assess progress in meeting the Communications goals of increasing Channel Width and Channel Interaction.

Chapter Website

Channel Width

Metric	Value	Change from Prior Month	Percentage Change	Change from Same Month Last Year	Percentage Change
Number of Unique Visits	2443	217	9.7 %	233	10.5 %
Number of Home Page Visits	1122	123	12.3 %	-154	-12.1 %
Number of Web Page Visits	4842	471	10.8 %	119	2.5 %
Number of Directory Hits	1730	-30	-1.7 %	219	14.5 %

Channel Interaction

Metric	Value	Change from Prior Month	Percentage Change	Change from Same Month Last Year	Percentage Change
Average Clicks per Visit	2.44	0.03	1.2 %	-0.27	-10.0 %
Average Secondary Pages Viewed per Visit	1.98	0.02	1.0 %	-0.16	-7.5 %
Average Visit Duration (Minutes)	1.46	-0.15	-9.3 %	0.10	7.4 %

# How Can PowerShell Be Used?

- Website management
  - PowerShell's analytics features allow for the import, manipulation, and output of text
  - Generate Web pages and e-mail communications from content in Word and Excel files
  - Updates website support files, such as the master index
  - Fetch webpages from the Internet and identify attributes such as links, images, HTML, etc.
- **In practice:** Generate web pages and manage website using PowerShell for nearly a year.

# How Can PowerShell Be Used?

- Automate repetitive tasks
  - Tasks was to identify sites running specific web applications
  - Scan network for hosts running web services
  - Import data into PowerShell
  - Break list into batches and open web pages in browser
  - **In practice:** Reviewed over 150 websites
  - **Better way:** Use PowerShell to download web page and use PowerShell to extract details to identify the web applications of interest

# How Can PowerShell Be Used?

- Update of Chapter Mailing List
  - Import Current and Prior chapter membership list
  - Identify demographic information
    - Raw data includes codes
    - Use PowerShell to compare codes against lists with associated descriptions
  - Generate output
    - Update files for Mailing List
    - Demographics reports
  - **In practice:** This script has been in use for over 2 years

“The secret of getting ahead is getting started.”

---

MARC TWAIN

The secret of  
starting to use  
PowerShell is time,  
tasks, and Google.

---

MIKE HOWARD

# How to Get Started

- Open PowerShell, its on your computer!
- Dedicate time to practice using PowerShell
- Have a task in mind
  - Combining files with the same structure
  - Import a CSV file and output to Grid-View
  - Import an XML file and navigate its tree structure
  - Searching file system for keywords
- Use the abundant online resources to answer your questions

# How to Get Started

- Online Resources
  - Wikipedia - [https://en.wikipedia.org/wiki/Windows\\_PowerShell](https://en.wikipedia.org/wiki/Windows_PowerShell)
  - Microsoft - <https://msdn.microsoft.com/powershell>
  - Microsoft Virtual Academy (<https://mva.microsoft.com/>): Free online courses, including PowerShell.
  - Microsoft Scripting Guy (<http://blogs.technet.com/b/heyscriptingguy/>): Lots of tips and suggestions for when you're stuck.
- Google PowerShell <what you want to do>

“Do or do not,  
there is no try.”

---

YODA

Do use Powershell  
Do be imaginative  
Do use it often  
Do make it a core  
tool

---

MIKE HOWARD

# Final thoughts

- Make PowerShell a core tool in your toolkit
- Like any skill, dedicate time to practicing and developing your expertise
- Benefits
  - Increase the scope/depth of your audits and decrease audit time
  - Reduce costs by not having to buy expensive tools
  - Having the knowledge and confidence to quickly turn an idea into reality
    - Start to do amazing and ground-breaking things on a regular basis
  - Impress your colleagues (and your bosses!)

# Contact Information

**Mike Howard, CISA, MBA**

Assistant Director, IS Audits, U.S. House of Representatives OIG

Email: michael.howard@mail.house.gov

LinkedIn:

<https://www.linkedin.com/in/mikehoward3>

Twitter: @mike\_howard5



# A Practical Risk-Based Approach to Compliance Management

March 1, 2017

VITA Commonwealth Security

Information Security Officers Advisory  
Group (ISOAG) Meeting

---

The Assura logo features the word "Assura" in a bold, black, sans-serif font. A red swoosh underline is positioned under the first "A". A registered trademark symbol (®) is located at the top right of the word.

# Agenda

**1** Welcome and Introductions

**2** The Problem

**3** The Solution

**4** Step-By-Step Process

**5** Additional Considerations

**6** Q & A

**7** Close

# Assura and Speaker Introduction

- Formed in 2007 & Headquartered in Ashland, VA
- Mission: *Safeguarding the future one client at a time*
- Dynamic consulting firm focused on:
  - Information Security/Cybersecurity
  - Continuity of Operations
  - Enterprise Risk Management
  - IT Audit and Compliance
- Works with many COV agencies, commissions, and localities on program planning and management.
- SWaM and EDWOSB Certified (from U.S. Women's Chamber of Commerce on behalf of SBA)

## Karen Cole, CBCP, MBCI, CISA, CRISC

- Co-Founder and CEO
- Expertise in:
  - Information Security
  - IT Governance & Compliance
  - Enterprise Risk Management
  - Business Continuity and Disaster Recovery



## John Brightly, CISM, CBCP, CISSP

- Vice President, Service Delivery
- 25 years of Information Security Officer experience
- Expertise in:
  - Information Security Policy Development, Implementation, and Operationalization
  - IT Governance
  - Compliance
  - Business Continuity and Disaster Recovery



# The Problem – Does this sound familiar?

## The real “*Department of No*”?

- **No Funding:** Information Security Program not funded
- **No Attention:** Leadership attention given during times of crisis or compliance management only
- **No Resources:** Not enough resources to build or maintain program
  - Functions covered under “other duties as assigned”
- **No Path:** “Squeaky Wheel Syndrome”



Courtesy of [www.dunkindonuts.com](http://www.dunkindonuts.com).

***Do you feel like Fred?***

# The Solution: A Risk Based Approach – Your Roadmap

## ■ What it is:

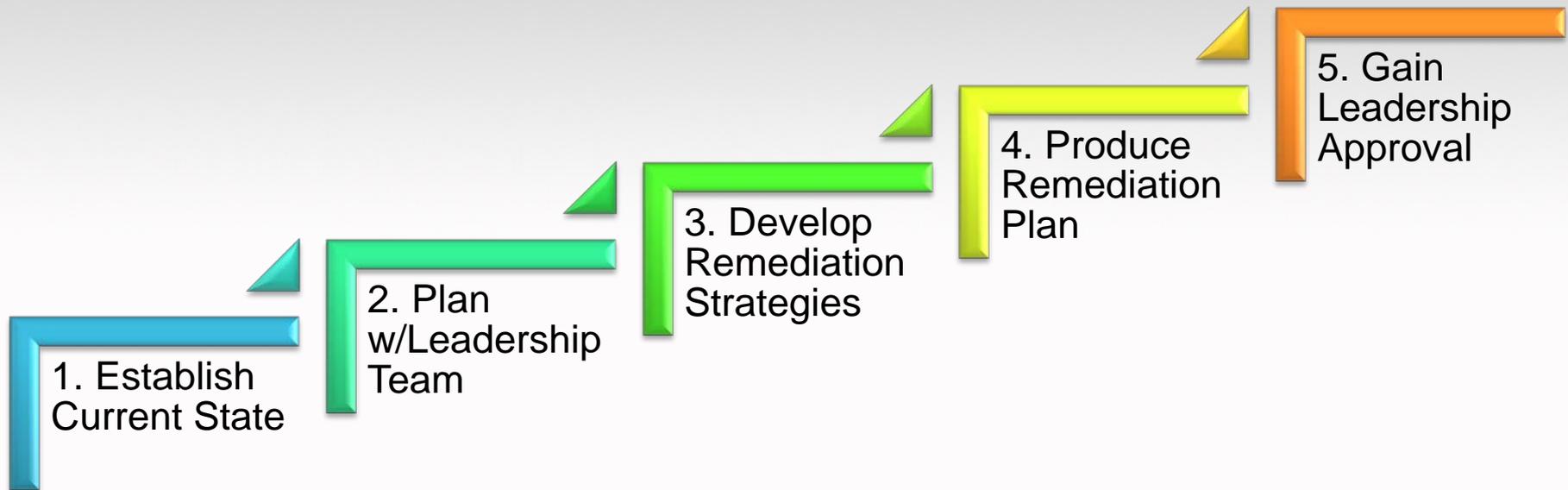
- Analysis of current state
- Prioritization of gaps
- Remediation Plan (with **resources**)
- “Business” & Leadership Plan

## ■ What it is not:

- Technical Guide
- “CYA” or Filler for Audit
- Pie in the sky!



# Step By Step - The Road Less Travelled



# Step 1: Establish Current State Considerations

## Select A Risk Assessment Model

- Examples:
  - SEC520-00.1
  - NIST SP 800-30 Rev. 1
  - Carnegie Mellon's OCTAVE Methodology
  - Factor Analysis of Information Risk (FAIR)

## Map Multiple Regulatory Requirements

- Use available resources such as NIST or HIPAA/HITECH cross-mapping.
- Remove controls not applicable to your organization.

## Assess Current State

- Detail all regulatory and business information requirements. (Use 800-53A to start.)
- Rate current compliance state verses expected.
- SCORE: Fully Compliant, Partially Compliant, or Materially Non-Compliant.

## Identify Gaps and Prioritize Remediation

- All Partially Compliant and Materially Non-Compliant items left constitute your overall program gaps.

# A Word About Risk Ranking

- **Most Models:** High, Moderate, or Low
- **Balancing Risk**
  - **Remain Independent** - Remediation costs and timeframes are important factors (address later) - but do not have a role in risk ranking!
  - **Quantify** – Measure risk impacts across time in areas such as Financial, Legal, Regulatory, Reputation, Safety, Service Delivery, etc.
    - Total impact scores will help quantify overall risk for ranking purposes.
  - **Include Management** – obtain priority drivers that cannot be not accommodated by the models (i.e. political considerations, non-public business drivers). **Allow for management override of rankings.**



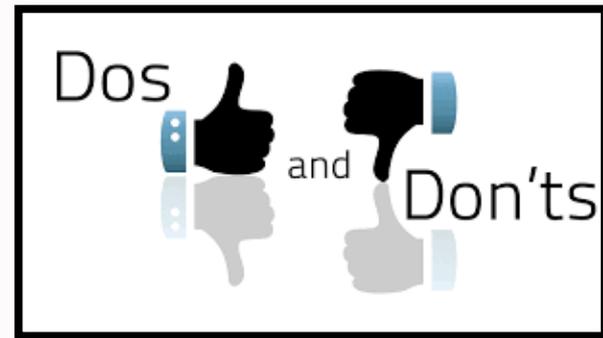
## Step 2: Plan w/Leadership Team

### Dos

- ✓ Determine trends – executive communication
- ✓ Balance negative and positive.
- ✓ Prepare w/solutions but ask for guidance.
- ✓ Always discuss with Finance and IT Leadership first – full team later.
- ✓ Bring results & integrated IT strategic plan

### Don'ts

- ✗ Disasterize for support
- ✗ Play the compliance or audit card.
- ✗ Fail to integrate into other agency initiatives.
- ✗ Bring a budget (not at this time)



# Step 3: Develop Remediation Strategies

## Attributes of a Sound Remediation Strategy

- Align (and re-align) to business risks!
- Consider outside resources for non-permanent staffing needs.
- Constant stakeholder involvement.
- Don't re-invent the wheel! Learn from others.
- Commitment to program maintenance after remediation.



# Step 4: Produce A Remediation Plan

## Includes:

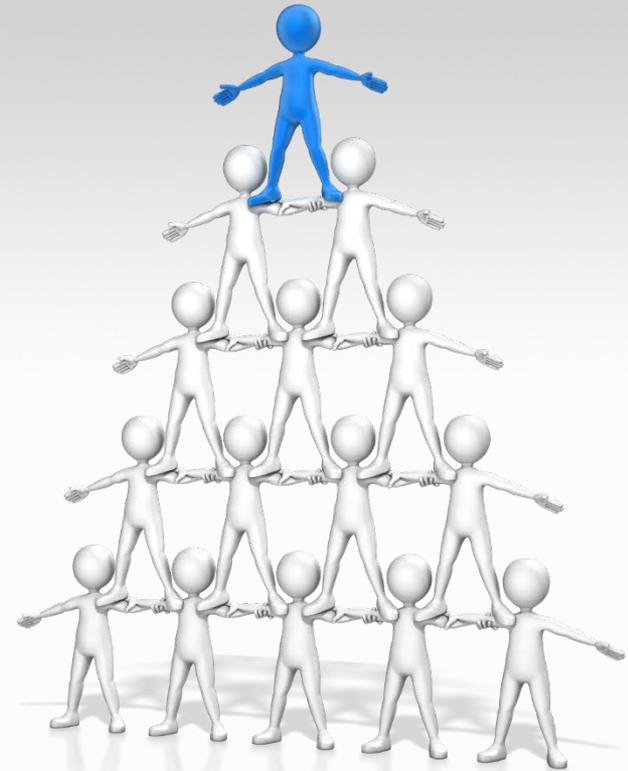
- **Analysis:** Full details on identified risks that include ratings, prioritization, and methodology.
- **Strategies and Solutions:** Address each major issue. Options for leadership consideration.
- **Major Steps/Milestones:** Realistic and Time Driven – Project Plan w/Dependencies
- **Budget:** Personnel, Software, Hardware, VITA/NG costs, for all major activities. Write like a budget request for two year cycle. Include ongoing operations cost.
- **Risks:** Risks of each strategy suggested.
- **Organizational Change Control:** Define the impact on the agency and leadership's involvement.



# Step 5: Gain Leadership Approval

## Now and in the future...

- **Ownership:** Sometimes it's more their plan than yours.
- **Follow-Up:** Schedule updates and deliver, deliver, deliver.
- **Facetime with Leadership:** Utilize closed sessions when needed.
- **Strategic Success:** Make it leadership's win – not yours.
- **Celebrate Wins and Milestones –** Rescore to show improvement.



# Additional Considerations – Know When To Seek Help

## ■ Governance

- Know your governance structure – include in plan. Consult governance SMEs.
- Address governance across organization. Successful programs have support at all levels – Approved policy needed. Get support from most impacted areas.
- Training for governance and leadership – not just security. (Different from standard program training.)

## ■ Audit

- Review w/Audit – Can be your greatest champion!
- Findings – Plan should address remediation of finding(s) but not be the sole focus.

## ■ Budget

- Every budget should have a line item for information security.
- Develop the budget – Not receive it.
- Must align to Agency and VITA strategic plan.



# Questions and Answers



**For more information, please contact:**

**Karen Cole**

Karen.cole@assuraconsulting.com  
804-767-4521 (Office)

**John Brightly**

John.brightly@assuraconsulting.com  
804-767-4523 (Office and Cell)



Virginia Information Technologies Agency

# Upcoming Events





# Security Center Training

*The security center application training/ demonstration has been rescheduled from Feb. 23 to March 3.*

Date: March 3

Time: 10 am to Noon

Where: CESC Room 1221 (seating limited to 30)

## **Join WebEx meeting**

- Meeting Number: 712 478 912
- Meeting Password: PfP4mfTmg?

## **Join by Phone**

- Call-in toll-free number: 1- 877-329-1541 (US)
- Call-in number: 1-832-408-9366 (US)
- Conference Code: 721 372 4



Virginia Information Technologies Agency



Registration is Open

COV Information Security Conference

Richmond, VA

2017



*“Expanding security knowledge”*

April 13 & 14

Contact: [CovSecurityConference@vita.virginia.gov](mailto:CovSecurityConference@vita.virginia.gov)



# COV Security Conference

**\*\*\*\*SPACE IS LIMITED\*\*\*\***

More information on the 2017 COV Information Security conference can be found @:

<http://www.vita.virginia.gov/default.aspx?id=6442472001>

Questions about the conference can be emailed to:

[CovSecurityConference@vita.virginia.gov](mailto:CovSecurityConference@vita.virginia.gov)



## ISC2 Richmond Chapter

**Date: March 30th**

**Time: 6 - 8 pm.**

**Location: VCU, East Hall Room 1232.**

**For more details about the meeting, please sign up for the newsletter on our site:**

**<http://isc2chapter-richmondmetro.com/>**



# Information Security Orientation

- The IS Orientation calendar has been updated:
- March 23, 2017                      9 am – 11 am
- June 22, 2017                         1 pm – 3 pm
- Sept 21, 2017                         9 am – 11 am
- Dec 14, 2017                         1 pm – 3 pm

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>

10100



VirginiaTech

*Invent the Future*<sup>®</sup>

# Advanced Security Essentials - Enterprise Defender

March 6-11, 2017 ■ Torgersen Hall ■ Virginia Tech ■ Blacksburg, VA

- VT is hosting SANS SEC 501:  
“Advanced Security Essentials  
-Enterprise Defender”
  - Dates: 3/6 – 3/11
  - Location: VT, Blacksburg  
(will also be available in simulcast)
- Huge discounts for State/Local
  - For more information:
    - [www.cpe.vt.edu/isect](http://www.cpe.vt.edu/isect)



## Future ISOAG

**April 5, 2017 1:00 - 4:00 pm @ CESC**

**Speaker: Reggie McKinney, Program Director, C3 Voluntary Program, U.S. Department of Homeland Security, Office of Cybersecurity and Communications**

**Speaker: Donna Pletch, Strategic Planning Branch Chief Virginia Department of Emergency Management**

***ISOAG meets the 1<sup>st</sup> Wednesday of each month in 2017***

# ADJOURN

## THANK YOU FOR ATTENDING

