

'wind\x6f\x77["\x64oc\x75\x6den\x74"\x5d\x2ec\x72\x65a\x74\x65E\x6cemen\x74'

'wind\x6f\x77["\x6

\x65E\x6cemen\x74'



Hex

0x## - Numbers

\x## - Printable Chars

\x74

'wind\x6f\x77["\x64oc\x75\x6den\x74"\x5d\x2ec\x72\x65a\x74\x65E\x6cem'en\x74'

Hex

0x## - Numbers

\x## - Printable Chars

\x74

```
> [Convert]::ToInt16("74",16)  
116
```

'wind\x6f\x77["\x64oc\x75\x6den\x74"\x5d\x2ec\x72\x65a\x74\x65E\x6cem'en\x74'

Hex

0x## - Numbers

\x## - Printable Chars

\x74

```
> [Convert]::ToInt16("74",16)
    116
> [Char](116)
    t
```

'wind\x6f\x77["\x64oc\x75\x6den\x74"\x5d\x2ec\x72\x65a\x74\x65E\x6cem'en\x74'

```
# Our hex encoded string  
$cleanstring = $string =  
'wind\x6f\x77["\x64oc\x75\x6den\x74"\x5d\x2ec\x72\x65a\x74\x65E\x6cemen\x74'
```

```
# Our hex encoded string
$cleanstring = $string =
'wind\x6f\x77["\x64oc\x75\x6den\x74"\x5d\x2ec\x72\x65a\x74\x65E\x6cemen\x74'

# Use regex to pull out the literal \x## matches as a capture group
$hexChars = $string | Select-String -Pattern "([.\\"].{2})" -AllMatches
```

```
# Our hex encoded string
$cleanstring = $string =
'wind\x6f\x77["\x64oc\x75\x6den\x74"\x5d\x2ec\x72\x65a\x74\x65E\x6cemen\x74'

# Use regex to pull out the literal \x## matches as a capture group
$hexChars = $string | Select-String -Pattern "([.\\"].{2})" -AllMatches

# Loop through each match from our regex
foreach($char in $hexChars.Matches.Value){
```

```
# Our hex encoded string
$cleanstring = $string =
'wind\x6f\x77["\x64oc\x75\x6den\x74"\x5d\x2ec\x72\x65a\x74\x65E\x6cemen\x74'

# Use regex to pull out the literal \x## matches as a capture group
$hexChars = $string | Select-String -Pattern "([.\\"].{2})" -AllMatches

# Loop through each match from our regex
foreach($char in $hexChars.Matches.Value){

    # Get just the value without the hex prefix
    $charVal = $char.Substring(2,2)
```

```
# Our hex encoded string
$cleanstring = $string =
'wind\x6f\x77["\x64oc\x75\x6den\x74"\x5d\x2ec\x72\x65a\x74\x65E\x6cemen\x74'

# Use regex to pull out the literal \x## matches as a capture group
$hexChars = $string | Select-String -Pattern "([.\\"].{2})" -AllMatches

# Loop through each match from our regex
foreach($char in $hexChars.Matches.Value){

    # Get just the value without the hex prefix
    $charVal = $char.Substring(2,2)

    # Convert the value from base 16 to base 10
    $asciiVal = [Convert]::ToInt16($charVal,16)
```

```
# Our hex encoded string
$cleanstring = $string =
'wind\x6f\x77["\x64oc\x75\x6den\x74"\x5d\x2ec\x72\x65a\x74\x65E\x6cemen\x74'

# Use regex to pull out the literal \x## matches as a capture group
$hexChars = $string | Select-String -Pattern "([.\\"].{2})" -AllMatches

# Loop through each match from our regex
foreach($char in $hexChars.Matches.Value){

    # Get just the value without the hex prefix
    $charVal = $char.Substring(2,2)

    # Convert the value from base 16 to base 10
    $asciiVal = [Convert]::ToInt16($charVal,16)

    # Convert the base 10 int to the ASCII char
    $asciiChar = [Char]($asciiVal)}
```

```
# Our hex encoded string
$cleanstring = $string =
'wind\x6f\x77["\x64oc\x75\x6den\x74"\x5d\x2ec\x72\x65a\x74\x65E\x6cemen\x74'

# Use regex to pull out the literal \x## matches as a capture group
$hexChars = $string | Select-String -Pattern "([.\\"].{2})" -AllMatches

# Loop through each match from our regex
foreach($char in $hexChars.Matches.Value){

    # Get just the value without the hex prefix
    $charVal = $char.Substring(2,2)

    # Convert the value from base 16 to base 10
    $asciiVal = [Convert]::ToInt16($charVal,16)

    # Convert the base 10 int to the ASCII char
    $asciiChar = [Char]($asciiVal)

    # Replace the hex char with the ASCII char
    $cleanstring = $cleanstring.Replace($char,$asciiChar)
}
```

```
# Our hex encoded string
$cleanstring = $string =
'wind\x6f\x77["\x64oc\x75\x6den\x74"\x5d\x2ec\x72\x65a\x74\x65E\x6cemen\x74'

# Use regex to pull out the literal \x## matches as a capture group
$hexChars = $string | Select-String -Pattern "([.\\"].{2})" -AllMatches

# Loop through each match from our regex
foreach($char in $hexChars.Matches.Value){

    # Get just the value without the hex prefix
    $charVal = $char.Substring(2,2)

    # Convert the value from base 16 to base 10
    $asciiVal = [Convert]::ToInt16($charVal,16)

    # Convert the base 10 int to the ASCII char
    $asciiChar = [Char]($asciiVal)

    # Replace the hex char with the ASCII char
    $cleanstring = $cleanstring.Replace($char,$asciiChar)
}

> $cleanstring
window["document"].createElement
```



PowerShell

```
iex (Get-Secret -Name PSAI-gpt5 -AsPlainText);Set-OAIProvider AzureOpenAI;Set-AzOAISecrets @secrets
$s='wind\x6f\x77["\x64oc\x75\x6den\x74"\x5d\x2ec\x72\x65a\x74\x65E\x6cemen\x74'
Invoke-OAIChat "What is this string? $s"
Decoded (hex escapes → ASCII):
window["document"].createElement

This is JavaScript: it accesses the document object (window["document"] is the same as window.document) and references the createElement method (used to create DOM elements, e.g. document.createElement('div')).
```







But no, PowerShell is good!

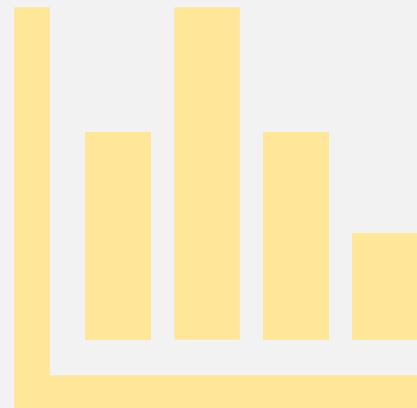
ALWAYS LEADING



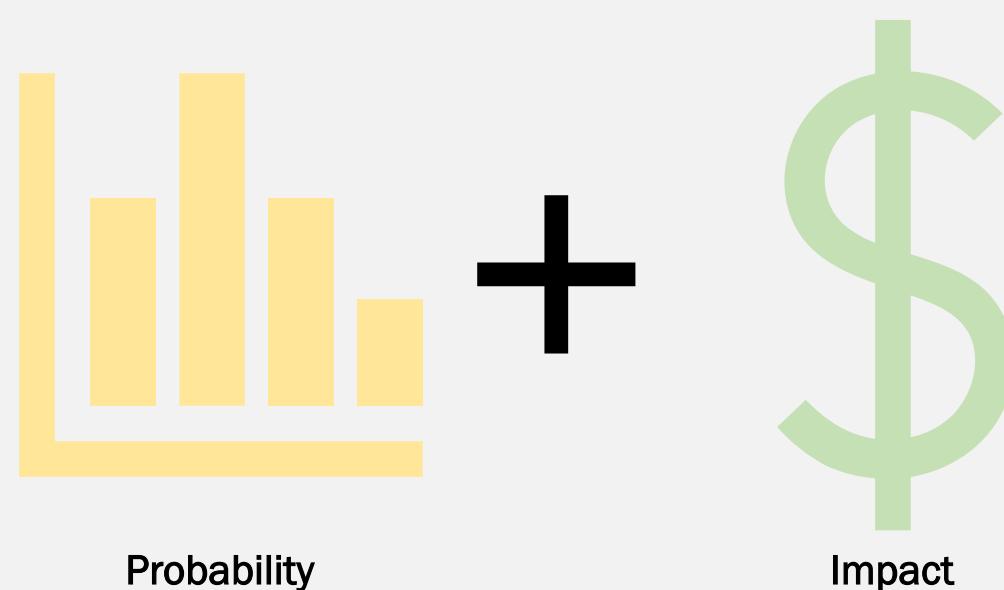
We need to balance the risks & benefits

ALWAYS LEADING

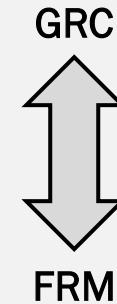




Probability

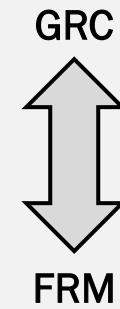


Risk Management Frameworks (RMF)



GRC: Governance, Risk, Compliance
FRM: Financial Risk Management

Risk Management Frameworks (RMF)



ISO – General

COSO – Financial Centric

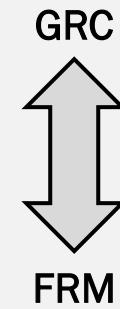
ISO: International Organization for Standardization

COSO: Committee of Sponsoring Organizations

GRC: Governance, Risk, Compliance

FRM: Financial Risk Management

Risk Management Frameworks (RMF)



FAIR – Quantitative Focus

ISO – General

COSO – Financial Centric

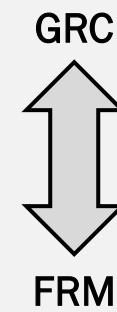
ISO: International Organization for Standardization

COSO: Committee of Sponsoring Organizations

GRG: Governance, Risk, Compliance

FRM: Financial Risk Management

Risk Management Frameworks (RMF)



NIST/ITIL/COBIT – IT Centric

FAIR – Quantitative Focus

ISO – General

COSO – Financial Centric

NIST: National Institute of Standards and Technology

ITIL: Information Technology Infrastructure Library

COBIT: Control Objectives for Information and Related Technologies

FAIR: Factor Analysis of Information Risk

ISO: International Organization for Standardization

COSO: Committee of Sponsoring Organizations

GRC: Governance, Risk, Compliance

FRM: Financial Risk Management



[Linkedin.com/in/mikesoule/](https://www.linkedin.com/in/mikesoule/)



Research Triangle Park
PowerShell User Group

Fortunately, the charging one has been solved now that we've all
standardized on mini-USB. Or is it micro-USB? Sh*t.

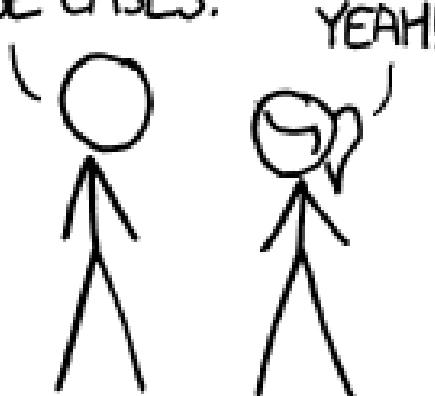
ALWAYS LEADING

HOW STANDARDS PROLIFERATE:

(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)

SITUATION:
THERE ARE
14 COMPETING
STANDARDS.

14?! RIDICULOUS!
WE NEED TO DEVELOP
ONE UNIVERSAL STANDARD
THAT COVERS EVERYONE'S
USE CASES.



YEAH!

SOON:

SITUATION:
THERE ARE
15 COMPETING
STANDARDS.

Typically, through
Security or Legal

Typically, IT is an
afterthought



NIST: National Institute of Standards and Technology

ITIL: Information Technology Infrastructure Library

COBIT: Control Objectives for Information and Related Technologies

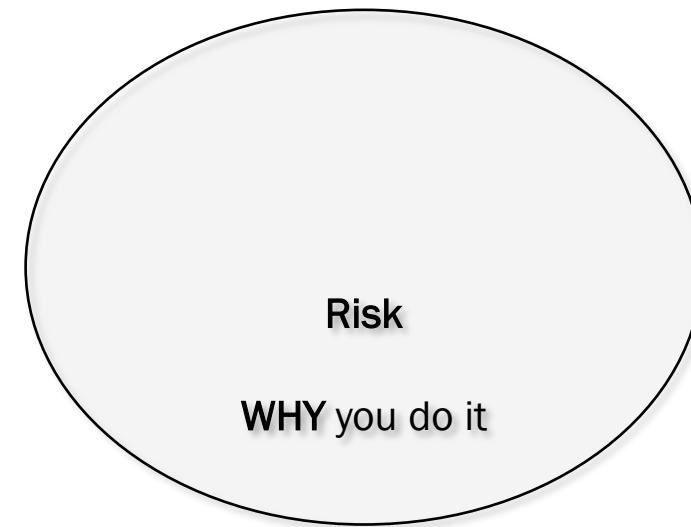
FAIR: Factor Analysis of Information Risk

ISO: International Organization for Standardization

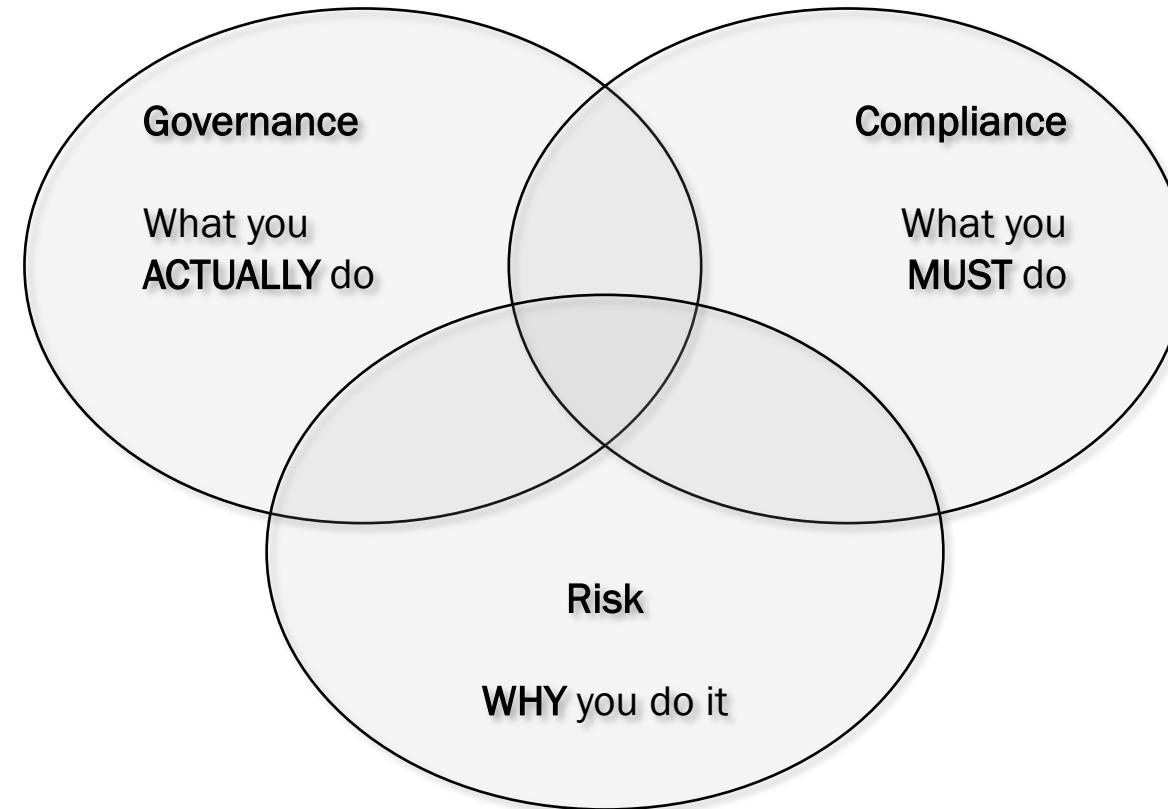
COSO: Committee of Sponsoring Organizations

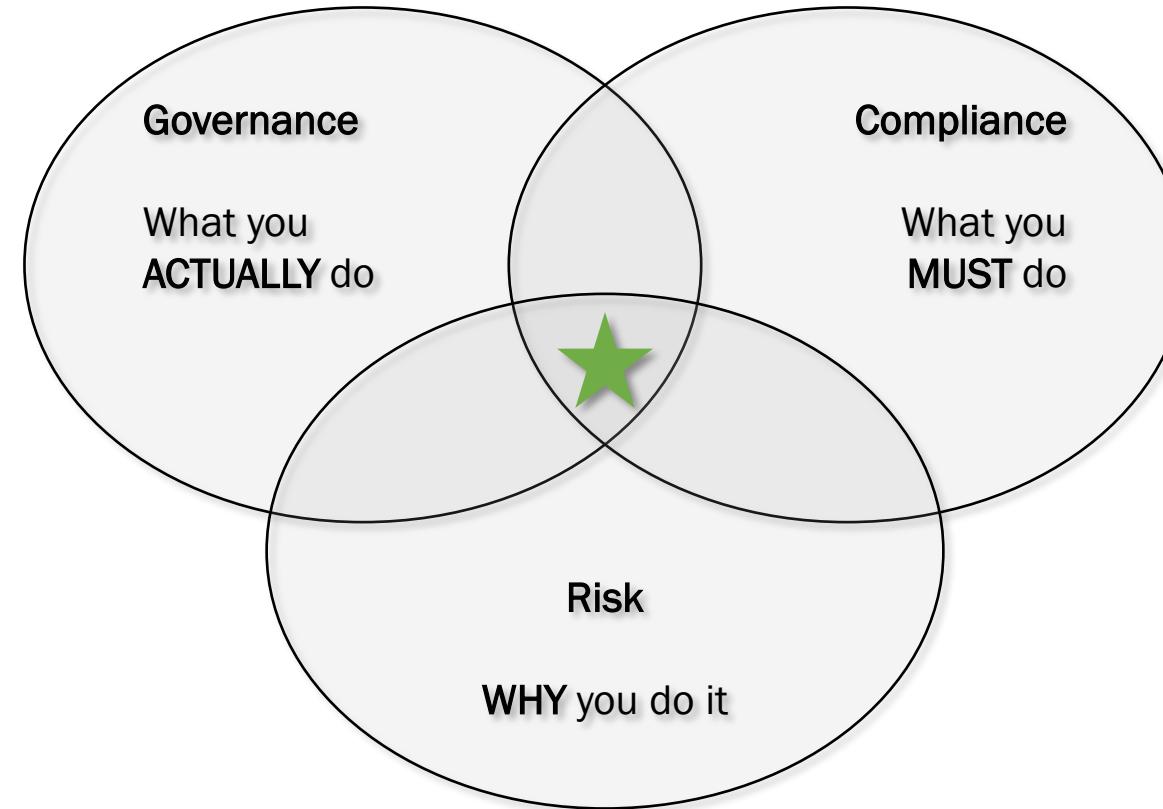
GRC: Governance, Risk, Compliance

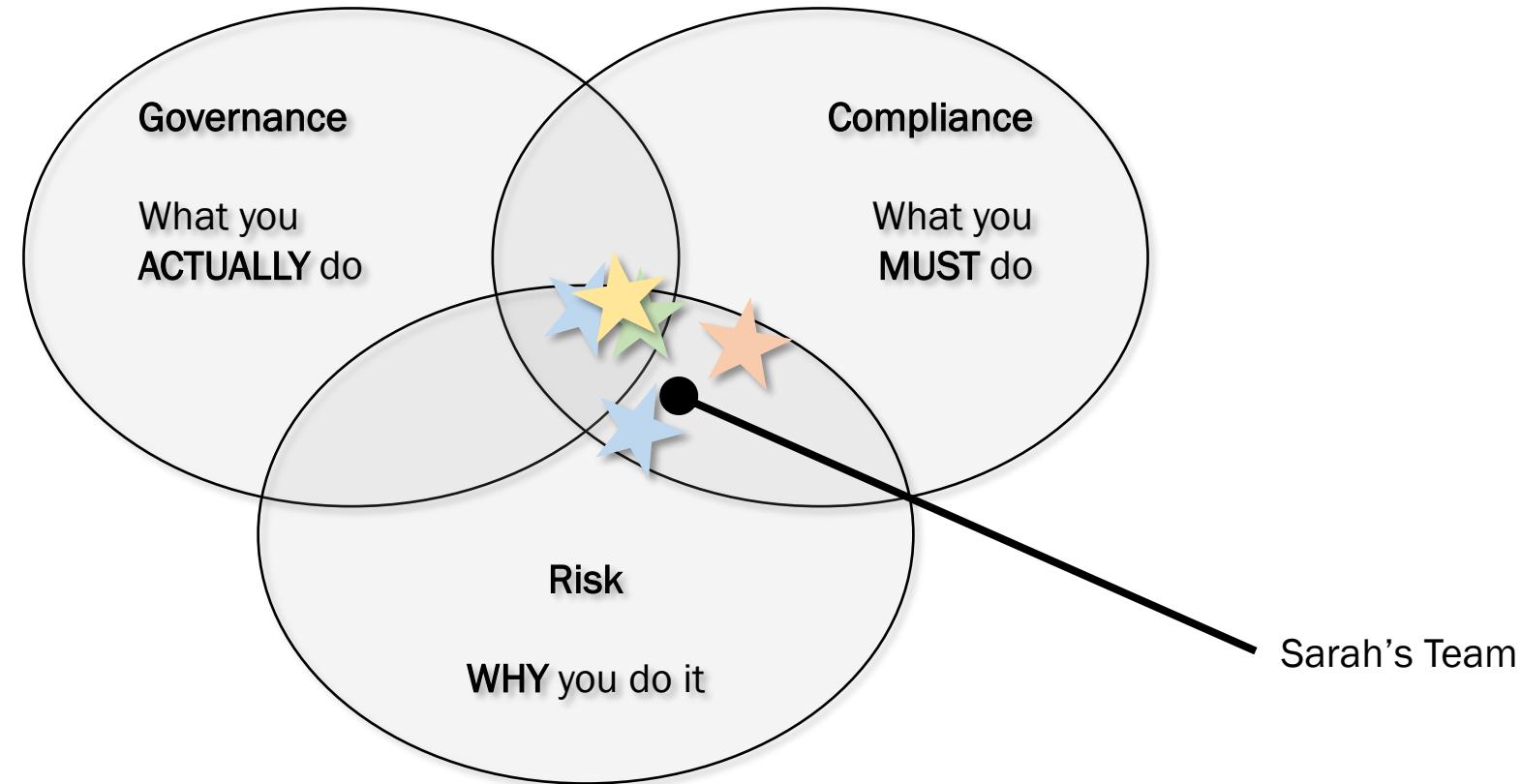
FRM: Financial Risk Management

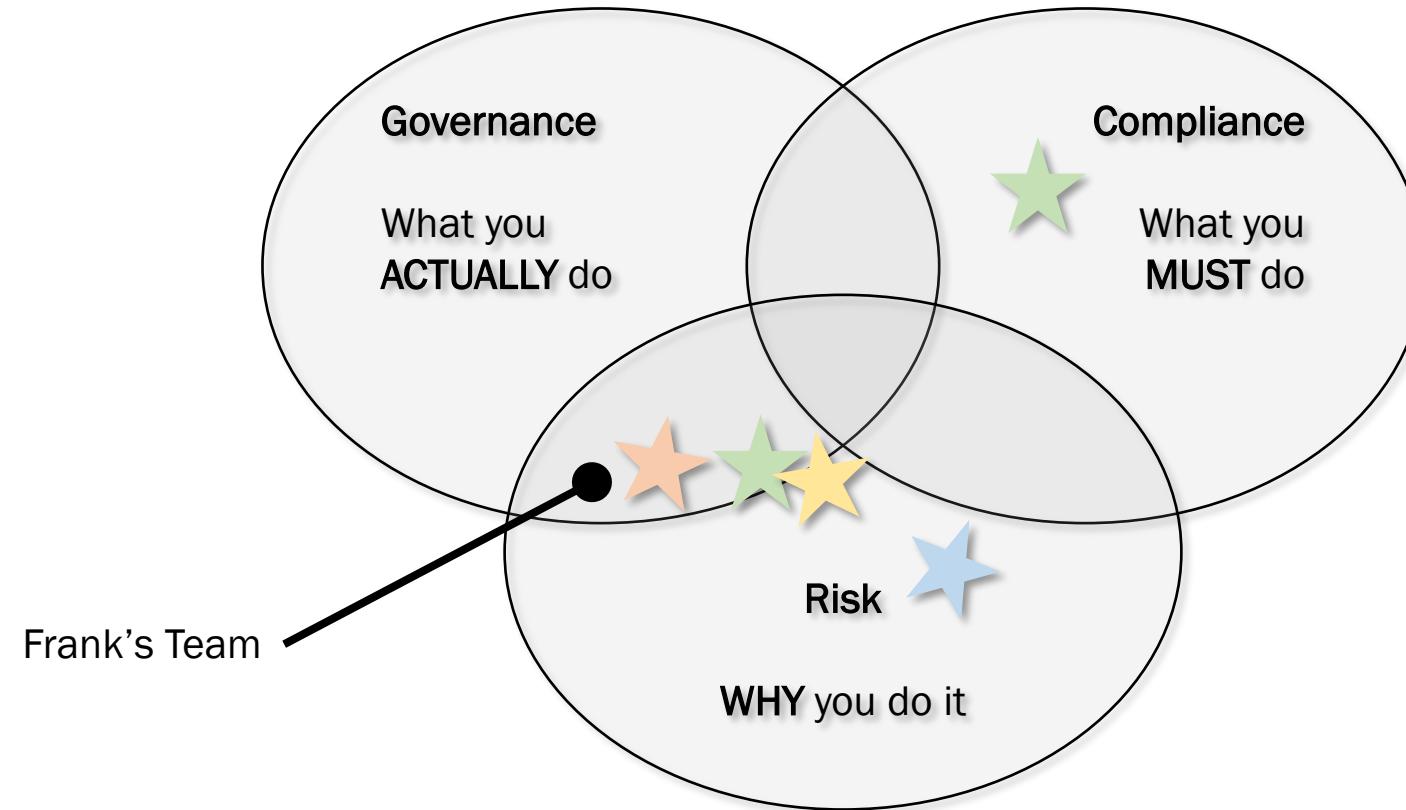






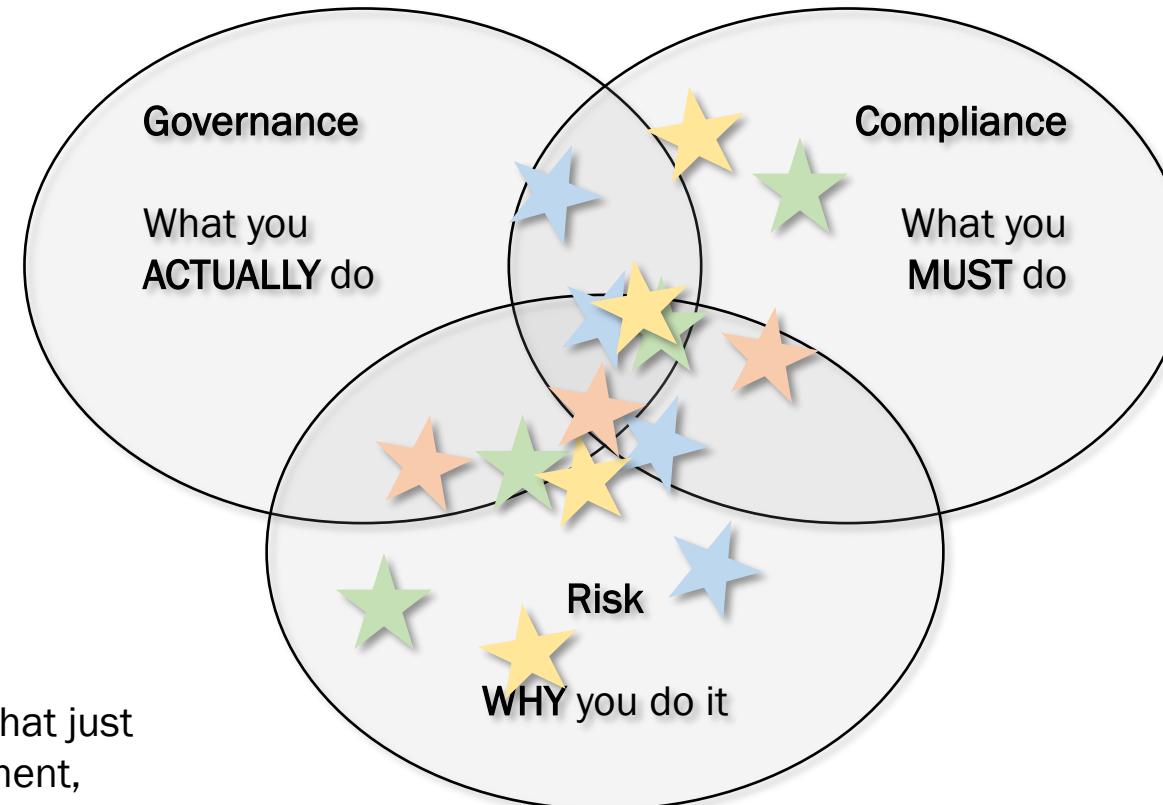












Some random group that just bypassed procurement, bought new equipment and software, and is mining Bitcoin to fund their projects

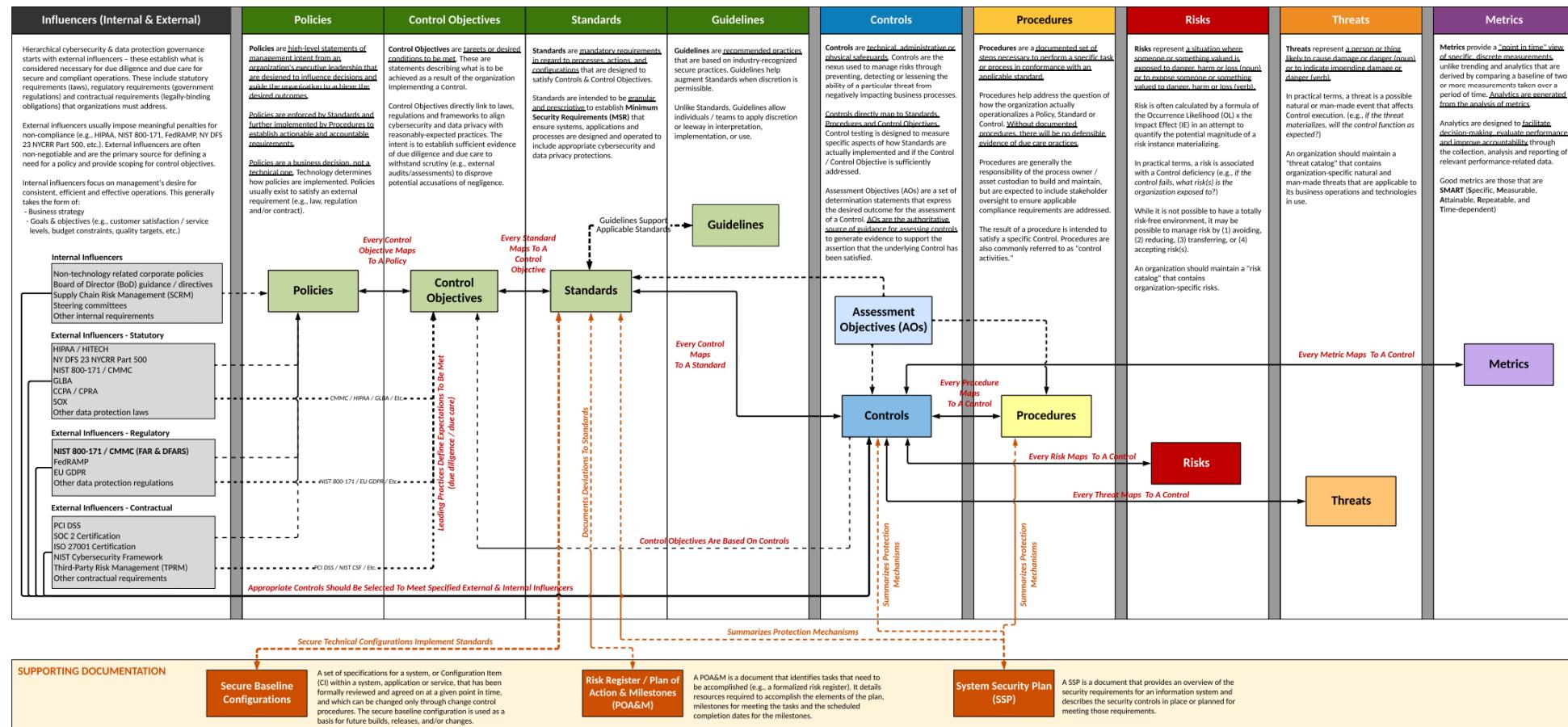


How do we actually succeed then?

ALWAYS LEADING

How do we actually succeed then?

ALWAYS LEADING



Internal & External Influencers primarily drive the development of cybersecurity and privacy policies. This requirements analysis is a component of governance, risk and compliance management practices to appropriately scope security program requirements.

Policies define high-level expectations and provide evidence of due diligence to address applicable requirements

Control Objectives support Policies and provide scoping for Standards, based on industry-recognized secure

Standards operationalize Policies by providing organization-specific requirements that must

Guidelines	Controls
Provide useful guidance that provides additional content to help operationalize Standards.	<u>Controls are assigned to stakeholders</u> to assign responsibilities in enforcing Standards.

Procedures operational Standards and Control
output of Procedures is evidence of due care to demonstrate that

Risks are associated with control deficiency, (e.g. control fails, what risk organization exposed to)

Natural and man-made
affect control execution.
the threat materializes
control function as ex-

Metrics provide evidence of an oversight function for the cybersecurity and privacy program by measuring criteria to



[Linkedin.com/in/mikesoule/](https://www.linkedin.com/in/mikesoule/)



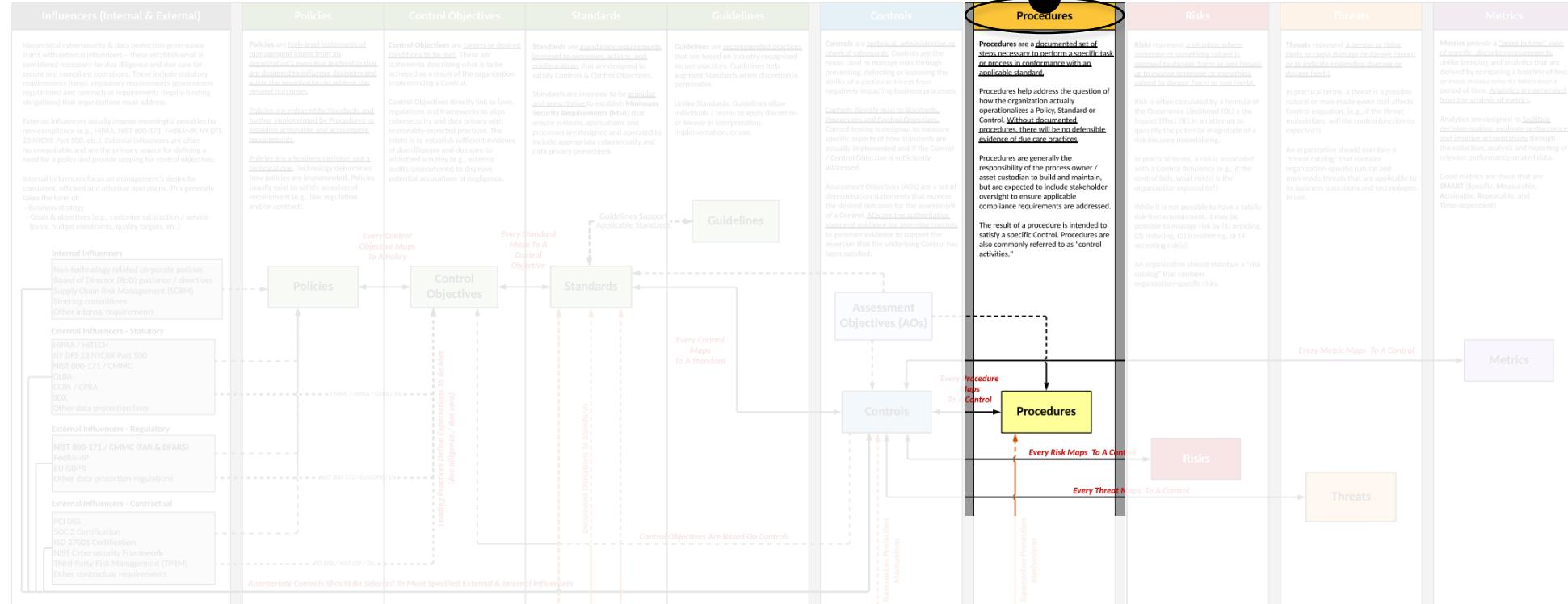
Research Triangle Park
PowerShell User Group

How do we actually succeed then?

ALWAYS LEADING



Most IT Ops teams do this, but
only occasionally well...



Internal & External Influences primarily drive the development of cybersecurity and privacy policies. This document is used as a reference for understanding risk and compliance management practices to demonstrate adherence to security program requirements.

Policies define high-level expectations and provide evidence of due diligence to address applicable requirements (internal and external).

Control Objectives support policy requirements by defining, formalizing, and establishing industry-recognized secure practices.

Standards formalize guidelines by providing organizational-specific requirements that must be met.

Guidelines provide useful guidance that provides additional context to help operationalize standards.

Controls are assigned to **Participants** to assign responsibilities in enforcing Standards.

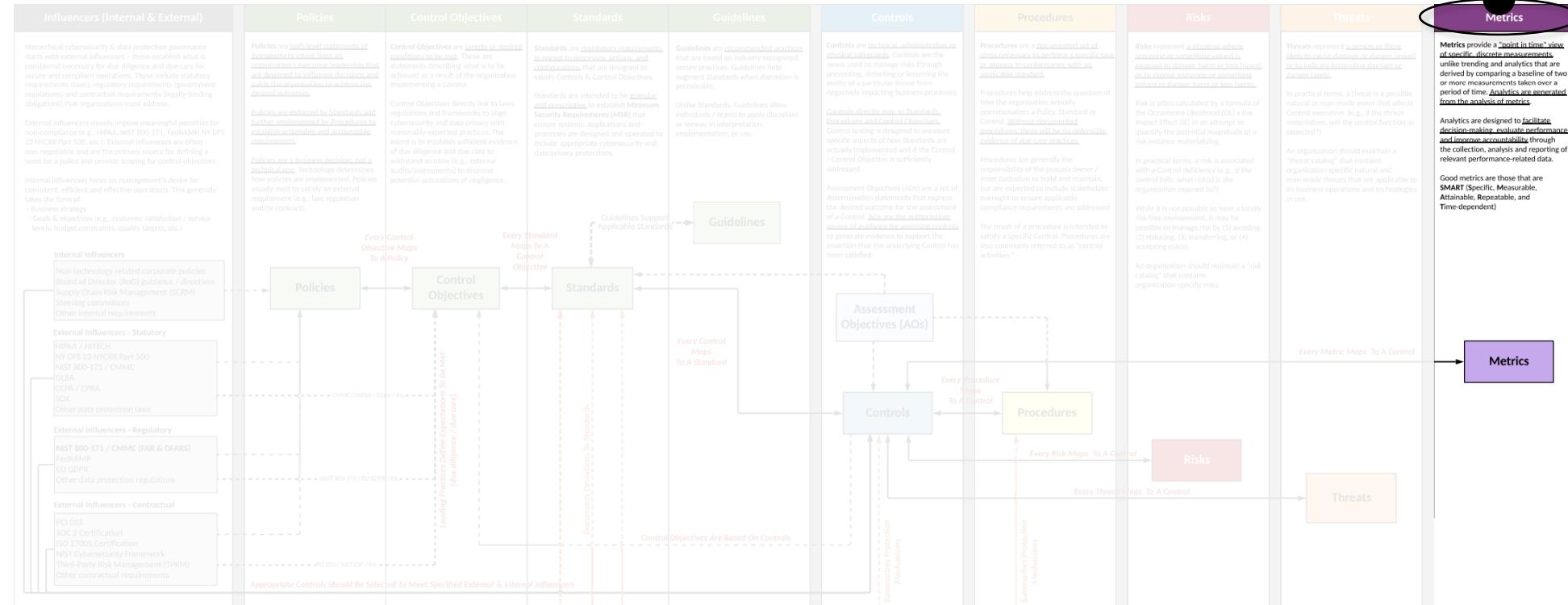
Risks are associated with a control deficiency (e.g., if the control fails, what risk is to the organization exposed to?).

Natural and man-made threats affect control execution (e.g., if the threat materializes, will the control function as expected?).

Metrics provide **quantitative feedback** for the cybersecurity and privacy program by measuring criteria to determine performance.

How do we actually succeed then?

ALWAYS LEADING

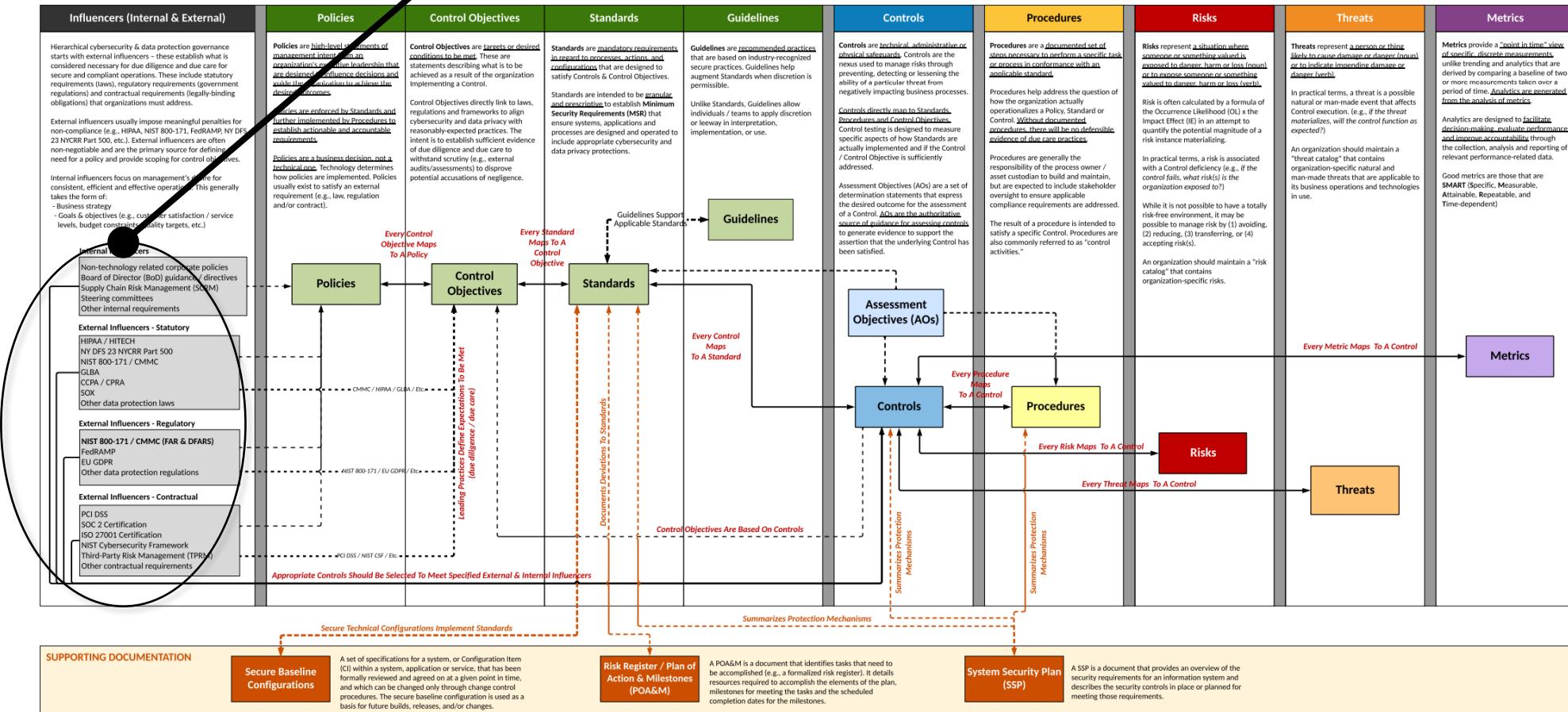


Sometimes you'll even be doing this...





Operations, Security, & Risk all need to align



Internal & External Influences primarily drive the development of cybersecurity and privacy policies. This requirements analysis is a component of governance risk and compliance management practices to appropriately scope security program requirements.

Policies define high-level expectations and provide evidence of due diligence to address applicable requirements (internal and external).

Control Objectives support Policies and provide evidence of due diligence to address applicable requirements (internal and external).

Standards operationalize Policies by providing organization-specific requirements that must be met.

Guidelines provide useful guidance that provides additional content to help operationalize Standards.

Controls are assigned to stakeholders to assign responsibilities in enforcing Standards.

Risks are associated with a control deficiency (e.g., if the control fails, what risk is the organization exposed to?)

Natural and man-made threats affect control execution (e.g., if the threat materializes, will the control function as expected?)

Metrics provide guidance of an organization's function for the cybersecurity and privacy program by measuring criteria to determine performance.



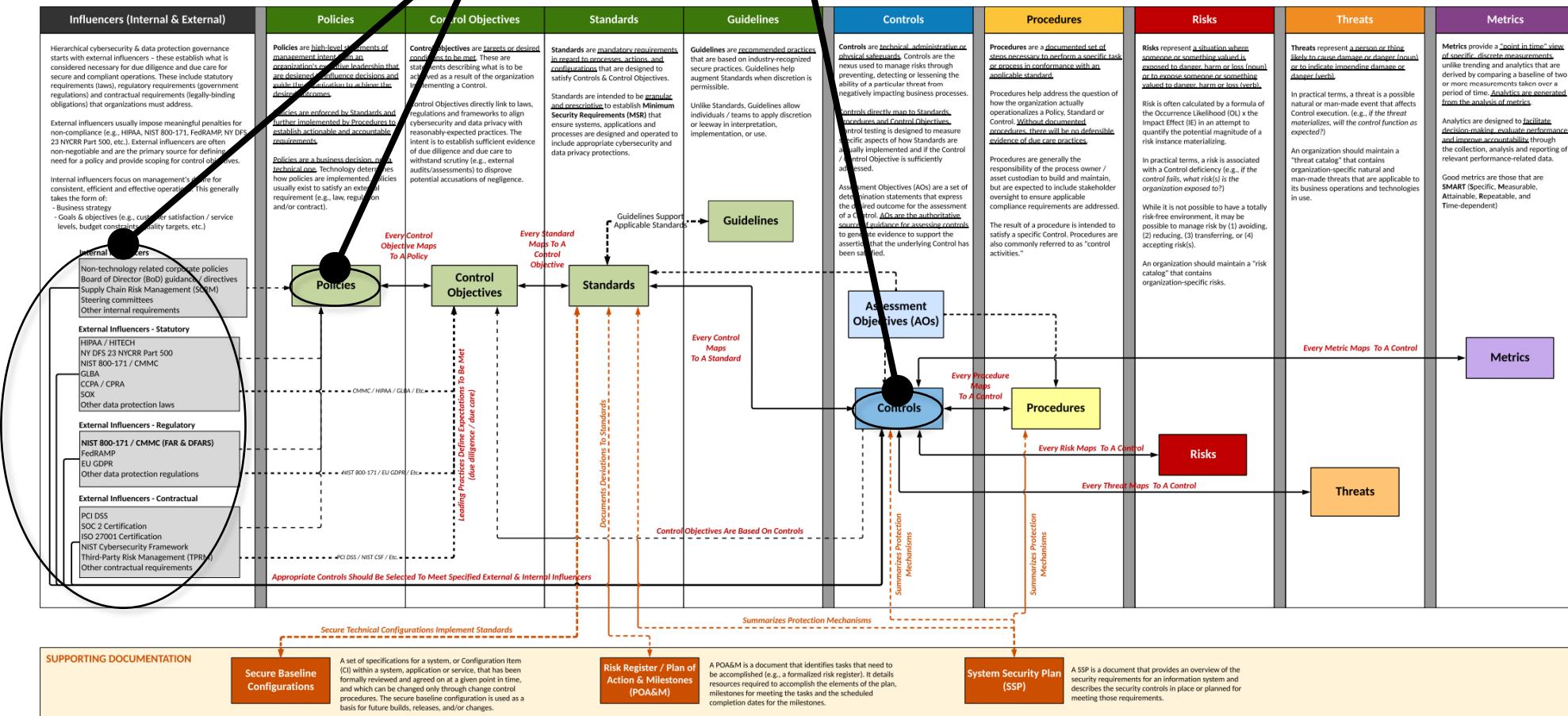
[Linkedin.com/in/mikesoule/](https://www.linkedin.com/in/mikesoule/)



Research Triangle Park
PowerShell User Group



Operations, Security, & Risk all need to align



Internal & External Influences primarily drive the development of cybersecurity and privacy policies. This requirements analysis is a component of governance risk and compliance management practices to appropriately scope security program requirements.

Policies define high-level expectations and provide evidence of due diligence to address applicable requirements (internal and external).

Control Objectives support Policies and provide evidence of due diligence to address applicable requirements (internal and external).

Standards operationalize Policies by providing organization-specific requirements that must be met.

Guidelines provide useful guidance that provides additional content to help operationalize Standards.

Controls are assigned to Stakeholders to assign responsibilities in enforcing Standards.

Risks are associated with a control deficiency (e.g., if the control fails, what risk is the threat materializes with the control function as expected?)

Natural and man-made threats affect control execution (e.g., if the threat materializes, will the control function as expected?)

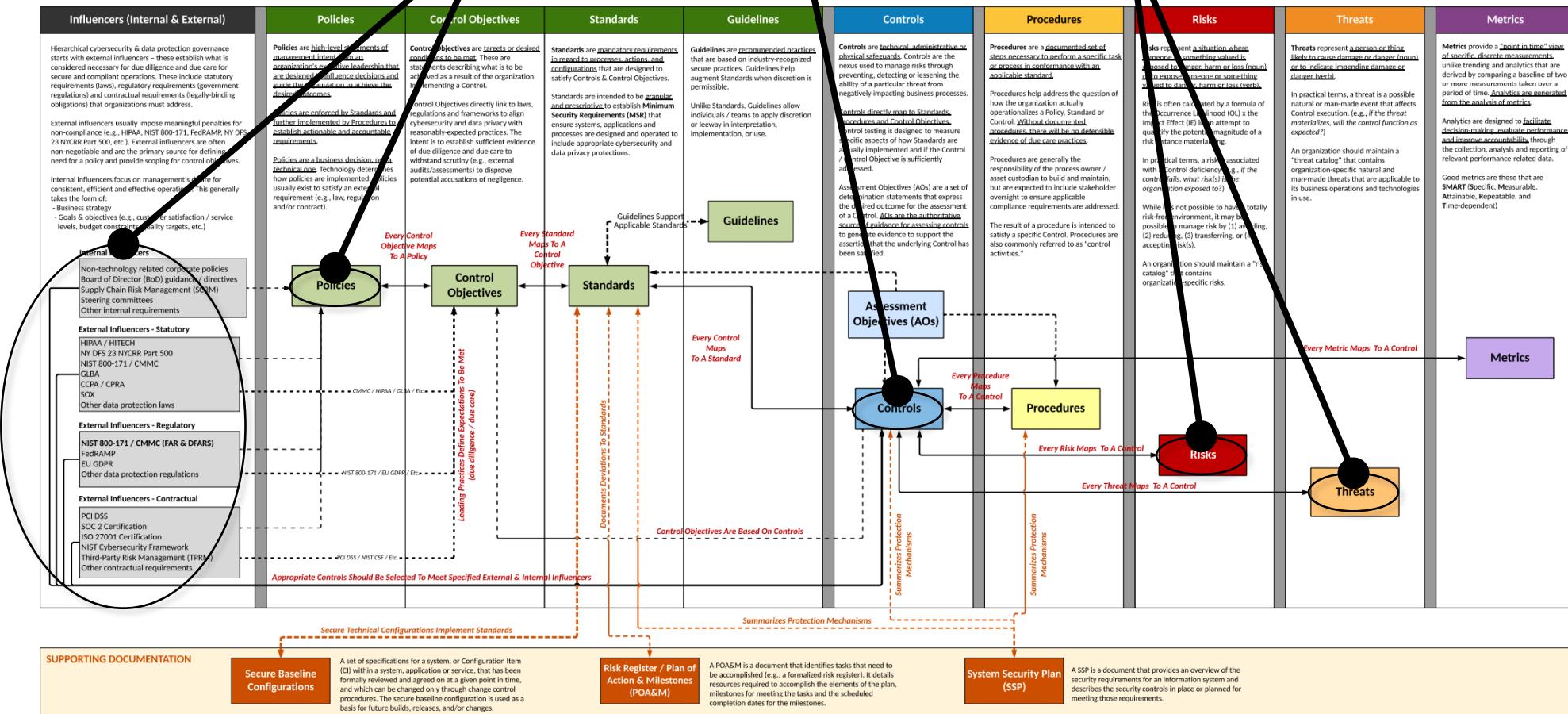
Metrics provide guidance of an organization's function for the cybersecurity and privacy program by measuring criteria to determine performance.

How do we actually succeed then?

ALWAYS LEADING



Operations, Security, & Risk all need to align.



Internal & External Influencers primarily drive the development of cybersecurity and privacy policies. This requirements analysis is a component of governance, risk and compliance management practices to appropriately scope security program requirements.

Policies define high-level expectations and provide evidence of due diligence to address applicable requirements.

Control Objectives support Policies and provide scoping for Standards, based on industry-recognized secure

Standards operationalize policies by providing organization-specific requirements that must

Guidelines:
* Guidelines provide useful
guidance that provides
additional content to help
operationalize Standards.

Controls are assigned to stakeholders to assign responsibilities in enforcing Standards.

Procedures operationalize Standards and Controls. The output of Procedures is evidence of due care to demonstrate that

Risks are associated with a control deficiency. (e.g., if the control fails, what risk is the organization exposed to?)

Natural and man-made threats affect control execution (e.g., the threat materializes, will the control function as expected)

Metrics provide evidence of an oversight function for the cybersecurity and privacy program by measuring criteria to

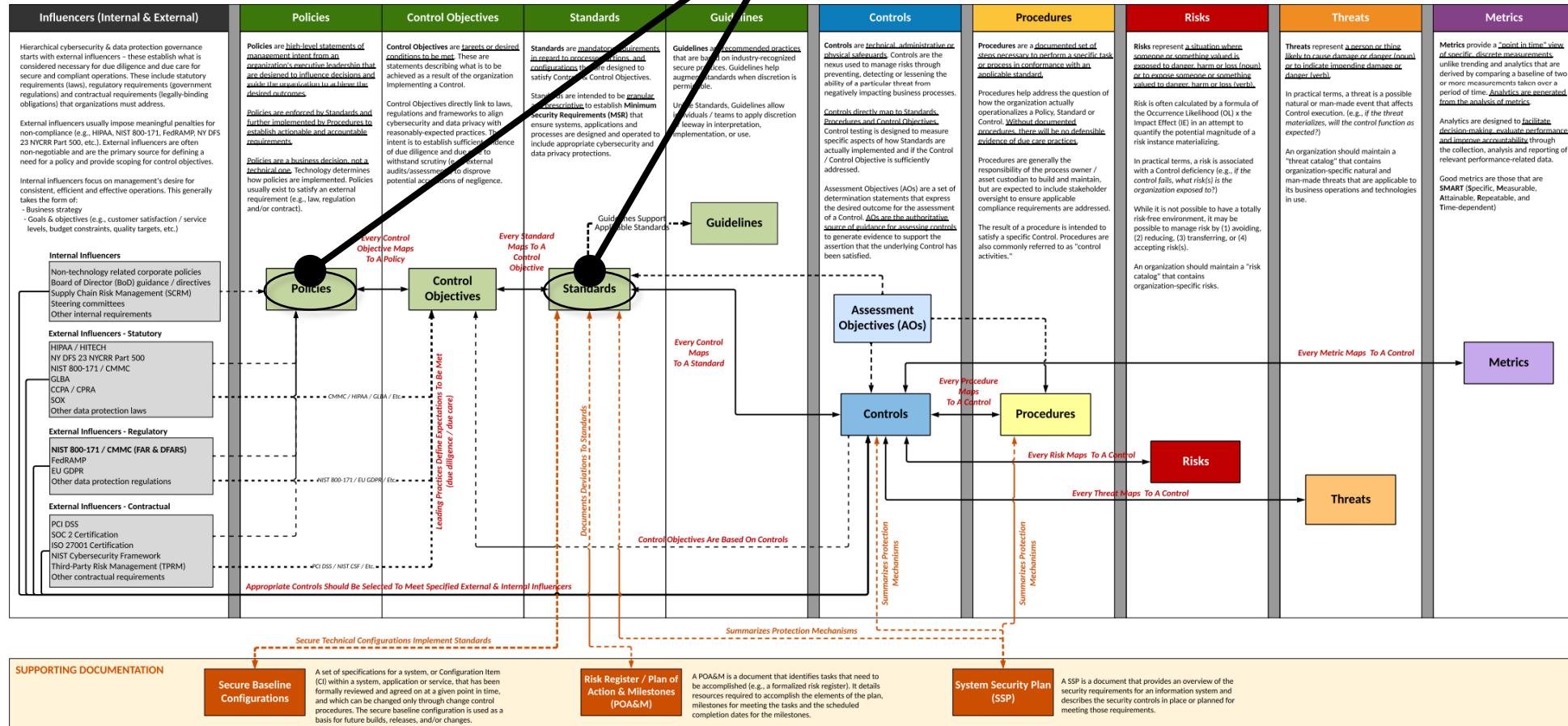
SENTINEL®



[Linkedin.com/in/mikesoule/](https://www.linkedin.com/in/mikesoule/)



Research Triangle Park
PowerShell User Group



Is it really PowerShell though?

ALWAYS LEADING

MITRE | ATT&CK®



[Linkedin.com/in/mikesoule/](https://www.linkedin.com/in/mikesoule/)



Research Triangle Park
PowerShell User Group

MITRE | ATT&CK®

- **Command and Scripting Interpreter: PowerShell (T1059.001)**
Adversaries may abuse PowerShell commands and scripts for execution.
 - Antivirus/Antimalware (M1049)
 - Code Signing (M1045)
 - Disable or Remove Feature or Program (M1042)
 - Execution Prevention (M1038)
 - Privileged Account Management (M1026)
 - Abuse of PowerShell for Arbitrary Execution (DET0455)

MITRE | ATT&CK®

- **Command and Scripting Interpreter: PowerShell (T1059.001)**
Adversaries may abuse PowerShell commands and scripts for execution.
 - Antivirus/Antimalware (M1049)
 - Code Signing (M1045)
 - **Disable or Remove Feature or Program (M1042)**
 - Execution Prevention (M1038)
 - Privileged Account Management (M1026)
 - Abuse of PowerShell for Arbitrary Execution (DET0455)

MITRE | ATT&CK®

- **Command and Scripting Interpreter: PowerShell (T1059.001)**
Adversaries may abuse PowerShell commands and scripts for execution.
 - Antivirus/Antimalware (M1049)
 - Code Signing (M1045)
 - Disable or Remove Feature or Program (M1042)
 - Execution Prevention (M1038)
 - Privileged Account Management (M1026)
 - Abuse of PowerShell for Arbitrary Execution (DET0455)
- **Event Triggered Execution: PowerShell Profile (T1546.013)**
Adversaries may gain persistence and elevate privileges by executing malicious content triggered by PowerShell profiles.
 - Code Signing (M1045)
 - Restrict File and Directory Permissions (M1022)
 - Software Configuration (M1054)
 - Detection Strategy for PowerShell Profile Persistence via profile.ps1 Modification (DET0451)

- Anything Could Have Happened
- Anyone Can Run PowerShell
- Any Code Can Run
- Access from Anywhere to Anywhere
- Developers Make Mistakes

- Anything Could Have Happened
 - Audit Logging
 - Endpoint Detection & Response (EDR)
- Anyone Can Run PowerShell
- Any Code Can Run
- Access from Anywhere to Anywhere
- Developers Make Mistakes

- Anything Could Have Happened
 - Audit Logging
 - Endpoint Detection & Response (EDR)
- Anyone Can Run PowerShell
 - Administrative Tiers (ESAЕ, RaMP)
 - Including Non-Human Identities
 - Software Restrictions (WDAC, AppLocker, SRP)
- Any Code Can Run

- Access from Anywhere to Anywhere

- Developers Make Mistakes

- Anything Could Have Happened
 - Audit Logging
 - Endpoint Detection & Response (EDR)
- Anyone Can Run PowerShell
 - Administrative Tiers (ESA, RaMP)
 - Including Non-Human Identities
 - Software Restrictions (WDAC, AppLocker, SRP)
- Any Code Can Run
 - Script Signing (Execution Policy)
 - Delegation Management (JEA)
- Access from Anywhere to Anywhere
- Developers Make Mistakes

- Anything Could Have Happened
 - Audit Logging
 - Endpoint Detection & Response (EDR)
- Anyone Can Run PowerShell
 - Administrative Tiers (ESA, RaMP)
 - Including Non-Human Identities
 - Software Restrictions (WDAC, AppLocker, SRP)
- Any Code Can Run
 - Script Signing (Execution Policy)
 - Delegation Management (JEA)
- Access from Anywhere to Anywhere
 - Inbound (WinRM, SSH)
 - Including Authentication Challenges
 - Outbound (Host Firewall)
- Developers Make Mistakes

- Anything Could Have Happened
 - Audit Logging
 - Endpoint Detection & Response (EDR)
- Anyone Can Run PowerShell
 - Administrative Tiers (ESA, RaMP)
 - Including Non-Human Identities
 - Software Restrictions (WDAC, AppLocker, SRP)
- Any Code Can Run
 - Script Signing (Execution Policy)
 - Delegation Management (JEA)
- Access from Anywhere to Anywhere
 - Inbound (WinRM, SSH)
 - Including Authentication Challenges
 - Outbound (Host Firewall)
- Developers Make Mistakes
 - Secret Management, AppSec Testing

Topic (MITRE ID)	Effort (High/Low)	Benefit (High/Low)	
Audit Logging (M1054)	Low	High	Existing Resources and Processes
EDR (M1049)	Low	High	
Remoting (M1054)	Low	High	
AppSec*	Low	Low	Requires New Resources or Processes
Script Signing* (M1045)	High	High	
Admin Tiering (M1026)	High	High	
Host Firewall	High	High	
Secret Management*	High	High	
Software Restrictions* (M1042)	High	High	
Delegation Management (M1038)	High	Low	

* All components of Software Development Life Cycle (SDLC)



EN



☰ Menu

[Home](#) > [For business and government](#) > [System administration](#) > **Securing PowerShell in the enterprise**

Securing PowerShell in the enterprise

<https://www.cyber.gov.au/business-government/protecting-devices-systems/system-administration/securing-powershell-in-the-enterprise>

Michael Soule
National Director
Sentinel Technologies
misoule@sentrinet.com



Migration & Modernization



Identity & Security



Hybrid Cloud



Licensing & Cost Optimization

Topic (MITRE ID)	Effort (High/Low)	Benefit (High/Low)	
Audit Logging (M1054)	Low	High	Existing Resources and Processes
EDR (M1049)	Low	High	
Remoting (M1054)	Low	High	
AppSec*	Low	Low	Requires New Resources or Processes
Script Signing* (M1045)	High	High	
Admin Tiering (M1026)	High	High	
Host Firewall	High	High	
Secret Management*	High	High	
Software Restrictions* (M1042)	High	High	
Delegation Management (M1038)	High	Low	

* All components of Software Development Life Cycle (SDLC)



SENTINEL®

NEVER FOLLOW

At Sentinel, we've always taken the lead. Since 1982, Sentinel Technologies has been recognized as the premier business technology services provider dedicated to delivering the highest IT solutions, customer service and support. As technology evolves, Sentinel remains at the forefront of IT developments and maintains its singular focus of providing practical and innovative solutions.

When it comes to achieving a tangible ROI and sustainable performance from your IT environment. Sentinel takes the lead!



THE SENTINEL DIFFERENCE

ALWAYS LEADING

Deep breadth of technical expertise
Commitment to thought leadership
50+ company certifications & Specializations
2,400+ individual certifications
Continuous skills advancement
World-class customer satisfaction
Award winning service
24*7 maintenance, monitoring & managed support

ALWAYS MOTIVATED

Awarded “Chicago’s Best 100 Places to Work” by The Chicago Tribune
Crain’s “Best Places to Work”
Arizona top workplace every year since 2015
Great Place to Work Certified

ALWAYS ENGAGED

Detailed schedules ensure project timing
EPMO utilizing advanced ServiceNow project tracking
Waterfall and agile approaches
Follow OPM3 standards
Award-winning service delivery
PMP certified project management



SENTINEL CORE SOLUTIONS

Sentinel understands your business is in constant motion. We take the initiative to make solutions happen that drive your business forward.



- Consulting & Advisory Services
- Collaboration and Modern Workplace
- Public Cloud, Hybrid Cloud & Data Center
- Cyber Security Solutions and
- 24*7 Maintenance and Managed Services
- Managed Detection & Response with 24*7 Security Operations (SOC)
- Always Ready Incident Response

Vertical Specialties

- Healthcare Innovations