

**Hackers Use PowerShell, Disable It!**

**ALWAYS LEADING**

'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\x6cemen\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\x6cemen\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\x6cemen\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 "([.\\][.x]{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 "([.\\][.x]{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 "([.\\][.x]{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 "([.\\][.x].{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 "([.\\][.x]{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 "([.\\][.x].{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 "([.\\][.x].{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
```



A PowerShell terminal window titled "PowerShell" with standard window controls. The terminal shows a PowerShell script being executed, with each line preceded by a pink folder icon and a green checkmark icon. The script uses the `Get-Secret` cmdlet to retrieve a secret named `PSAI-gpt5`, sets the OpenAI provider to `AzureOpenAI`, and then uses `Invoke-OAIChat` to ask a question about a hex-encoded string. The output shows the decoded string, which is a JavaScript snippet. A final pink folder icon and green checkmark icon are shown at the bottom of the terminal.

```
iex (Get-Secret -Name PSAI-gpt5 -AsPlainText);Set-OAIProvider AzureOpenAI;Set-AzOAI Secrets @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!**

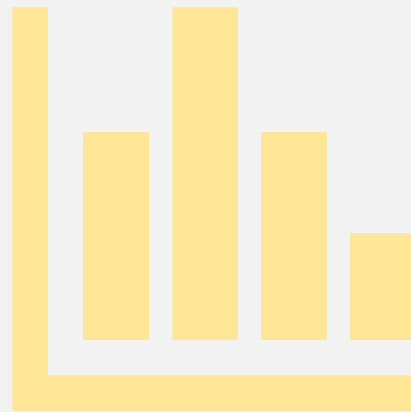
**ALWAYS LEADING**



**We need to balance the risks & benefits**

**ALWAYS LEADING**

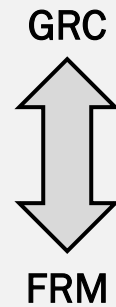




Probability



### Risk Management Frameworks (RMF)



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



ISO: International Organization for Standardization  
COSO: Committee of Sponsoring Organizations  
GRC: Governance, Risk, Compliance  
FRM: Financial Risk Management



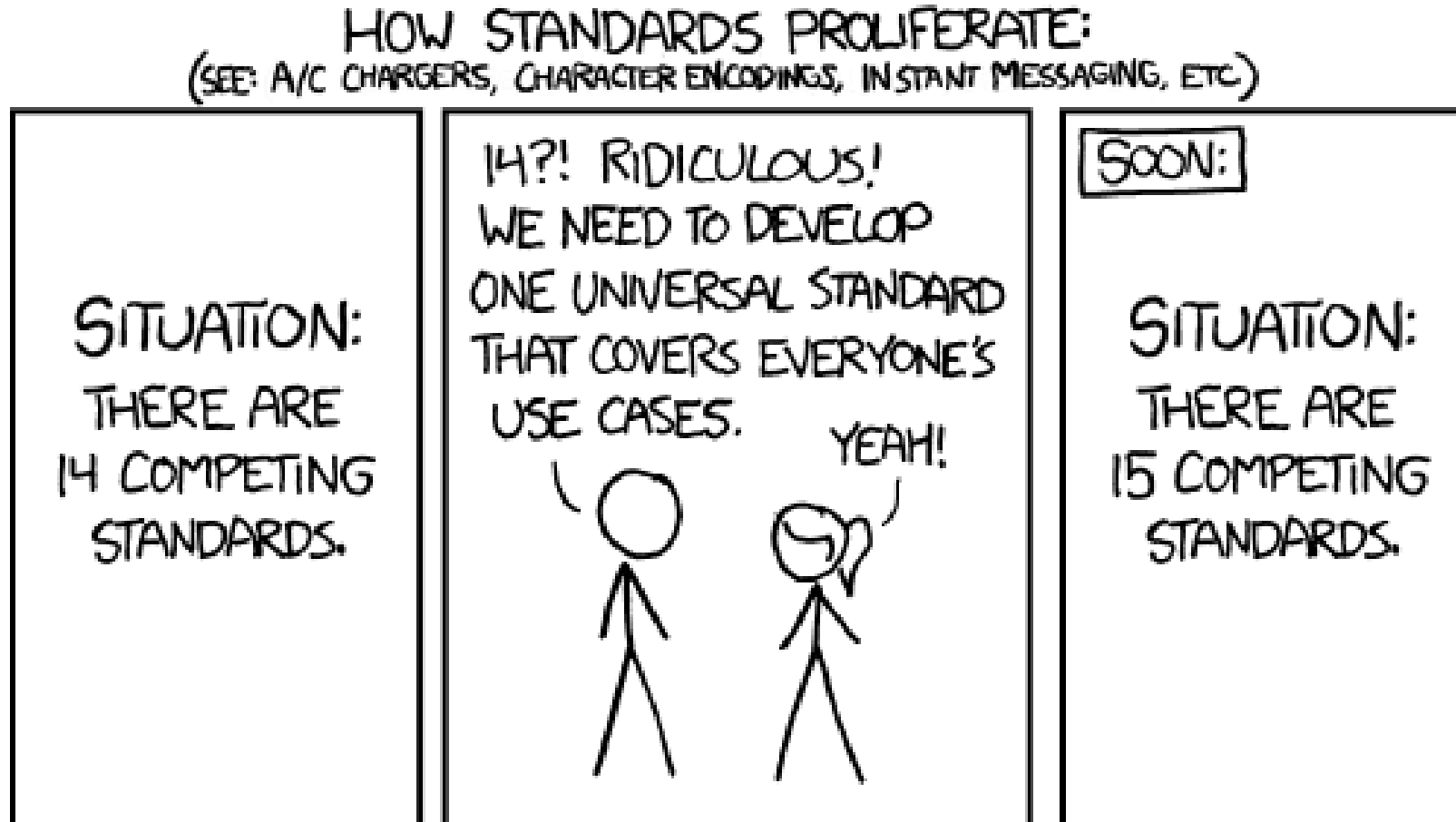




NIST: National Institute of Standards and Technology  
ITIL: Information Technology Infrastructure Library  
COBIT: Control Objectives for Information and Related Technologies  
FAIR: Factor Analysis of Information Risk  
ISO: International Organization for Standardization  
COSO: Committee of Sponsoring Organizations  
GRC: Governance, Risk, Compliance  
FRM: Financial Risk Management

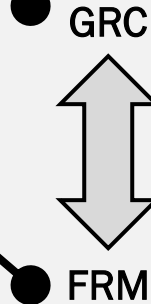
Fortunately, the charging one has been solved now that we've all standardized on mini-USB. Or is it micro-USB? Sh\*t.

ALWAYS LEADING



Typically, through  
Security or Legal

Typically, IT is an  
afterthought



### Risk Management Frameworks (RMF)

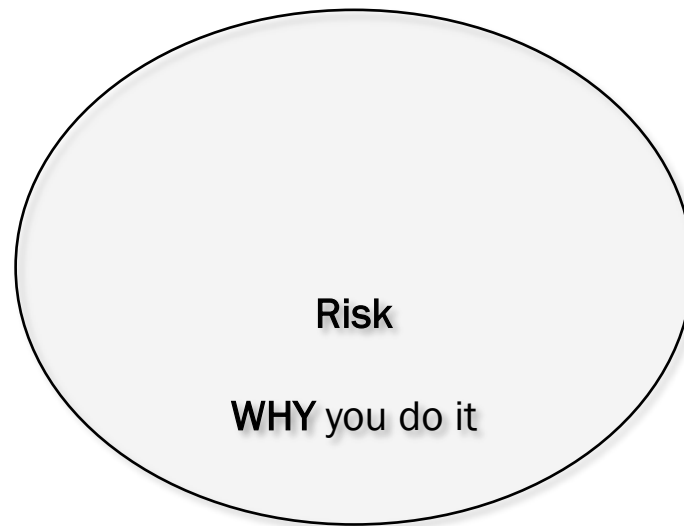
NIST/ITIL/COBIT – IT Centric

FAIR – Quantitative Focus

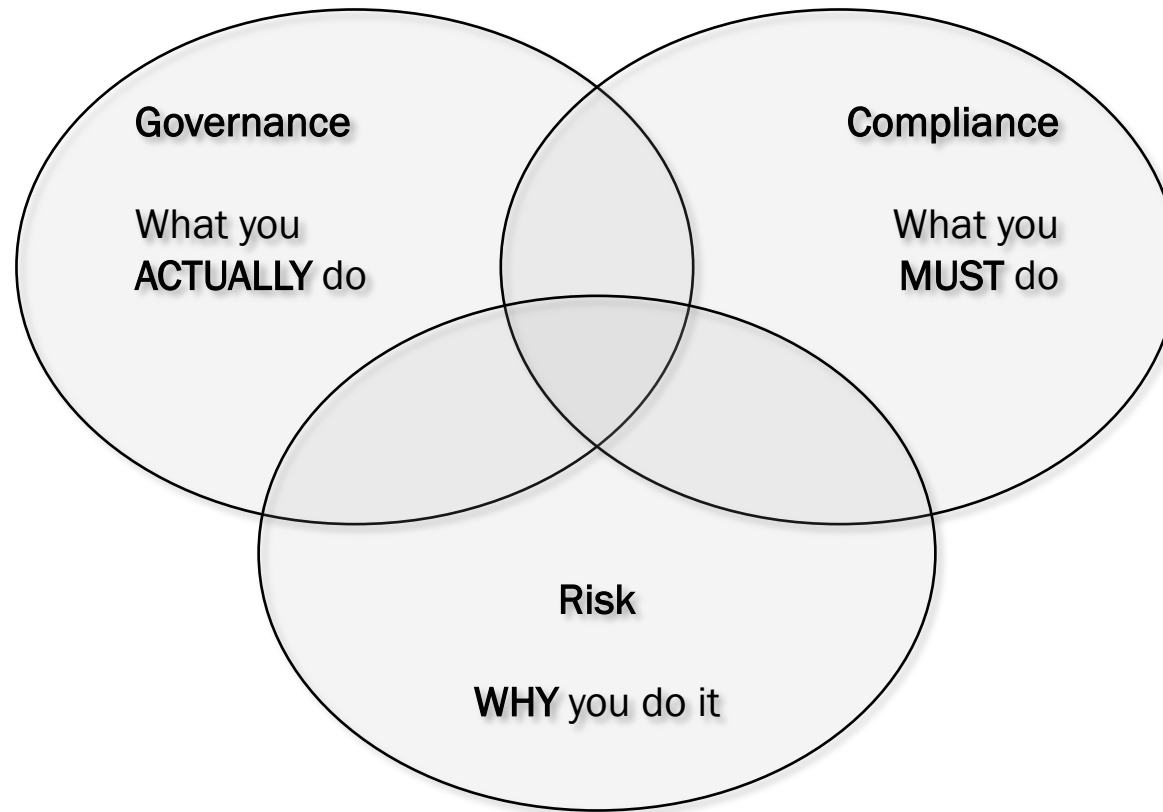
ISO – General

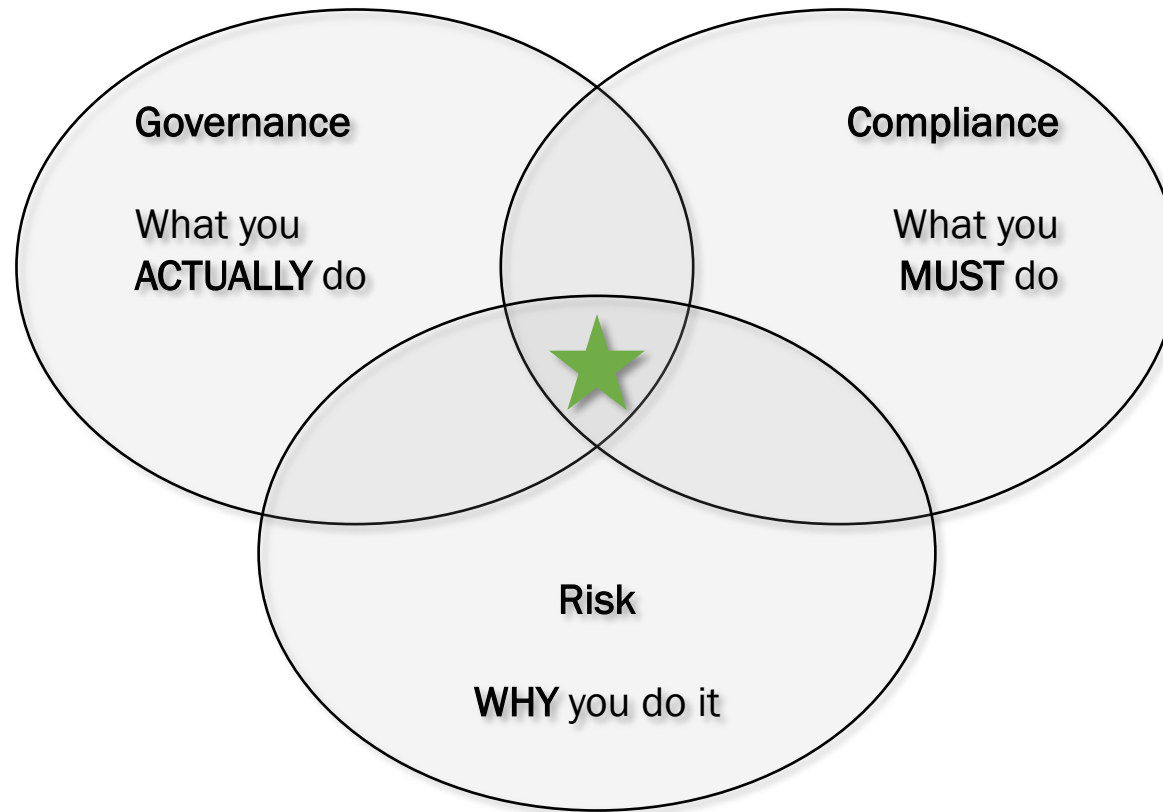
COSO – Financial Centric

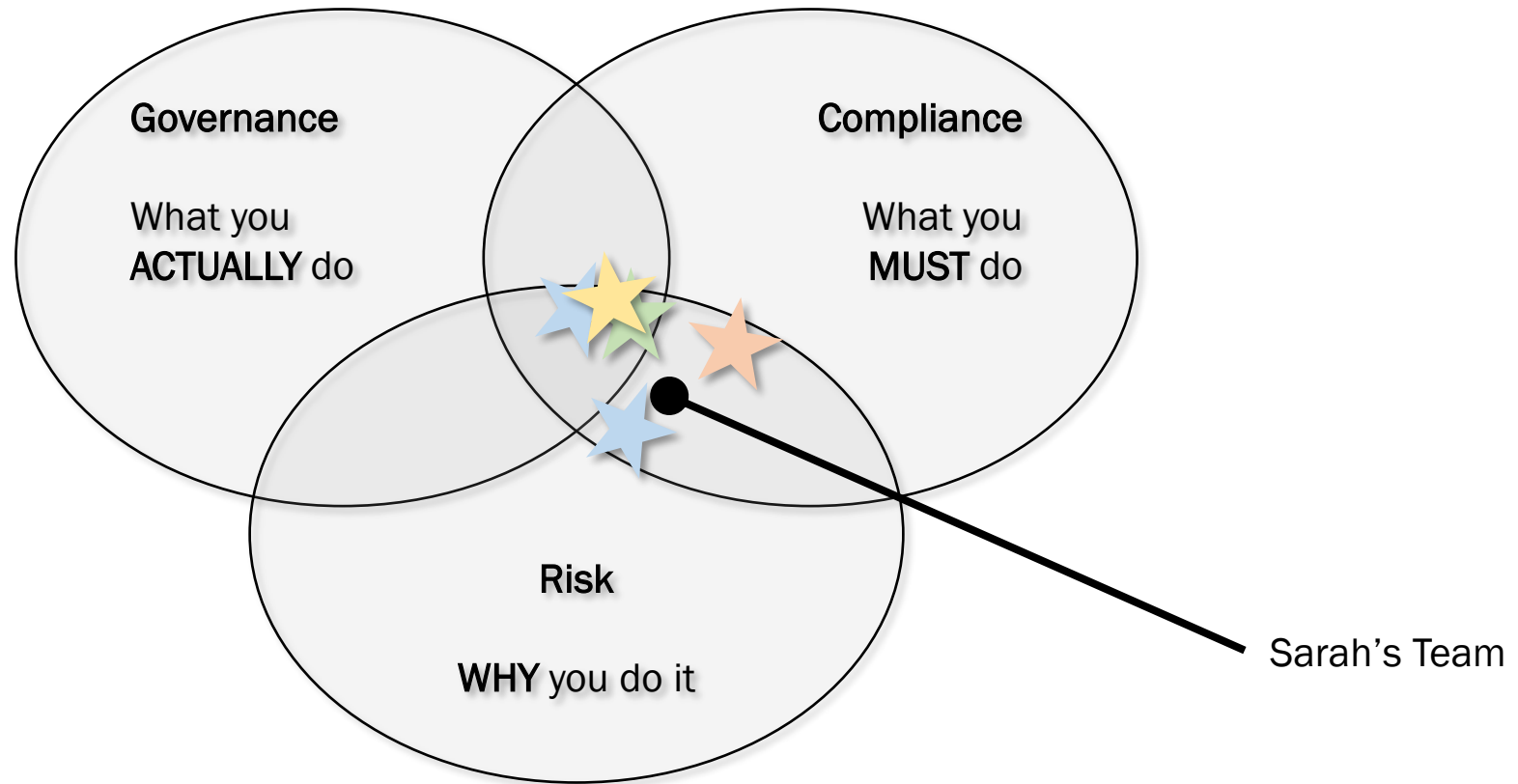
NIST: National Institute of Standards and Technology  
ITIL: Information Technology Infrastructure Library  
COBIT: Control Objectives for Information and Related Technologies  
FAIR: Factor Analysis of Information Risk  
ISO: International Organization for Standardization  
COSO: Committee of Sponsoring Organizations  
GRC: Governance, Risk, Compliance  
FRM: Financial Risk Management



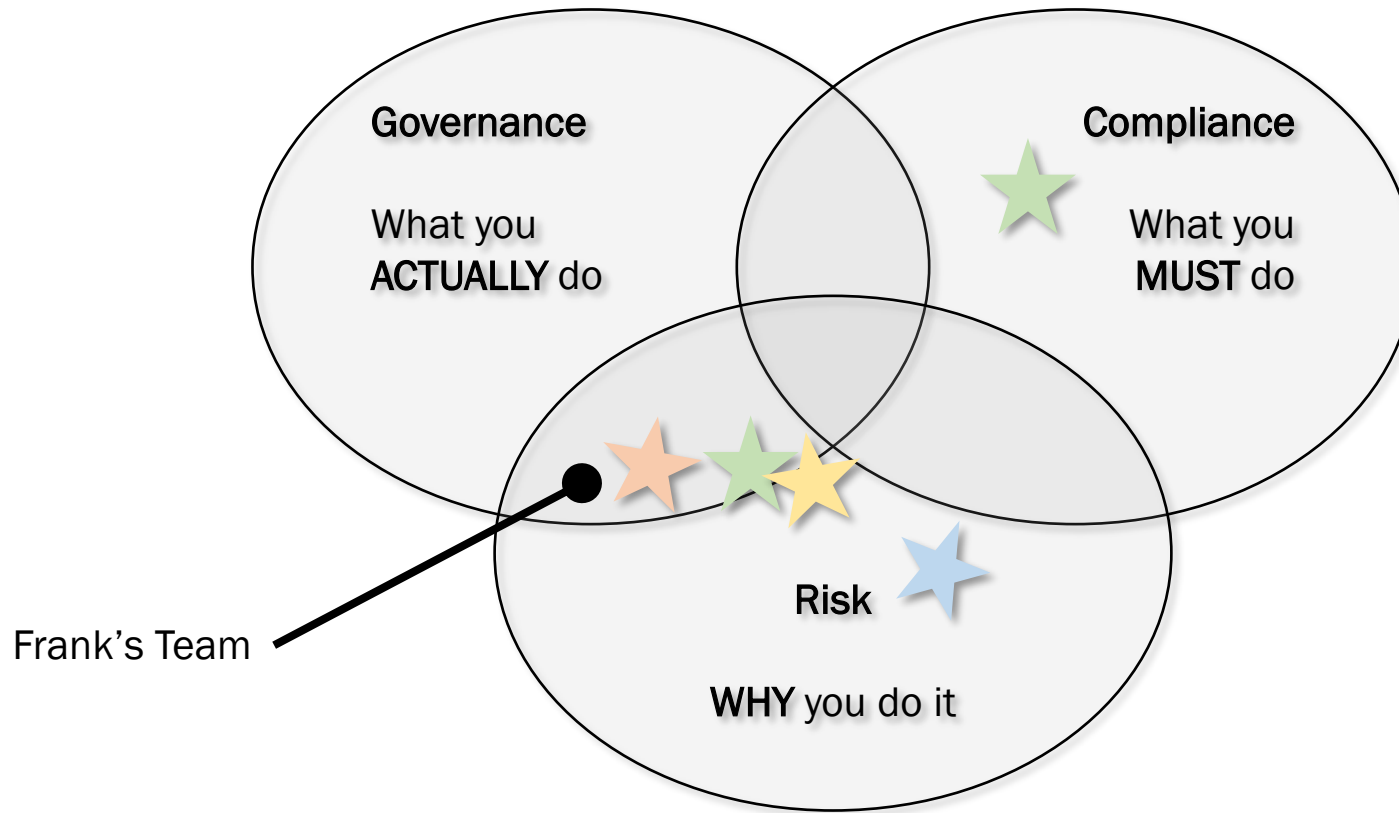


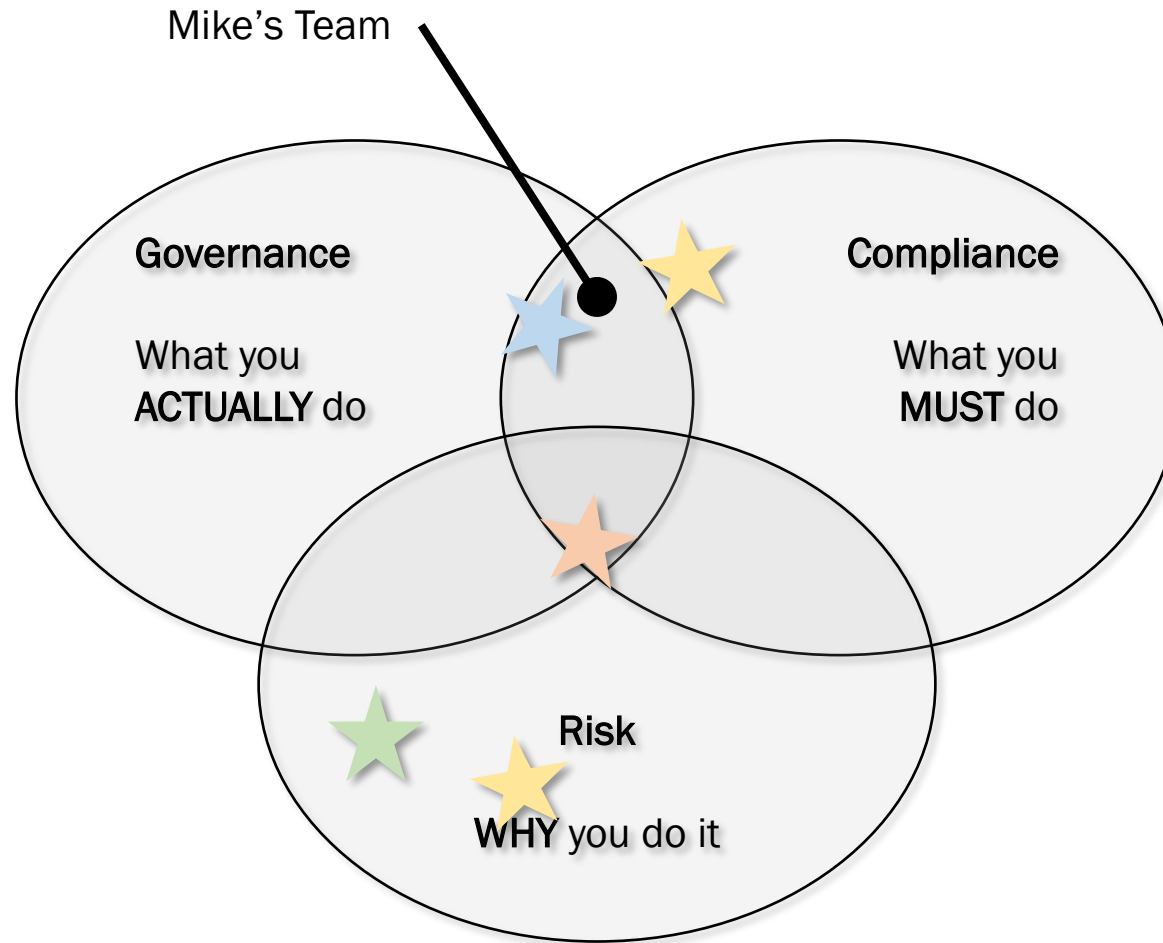




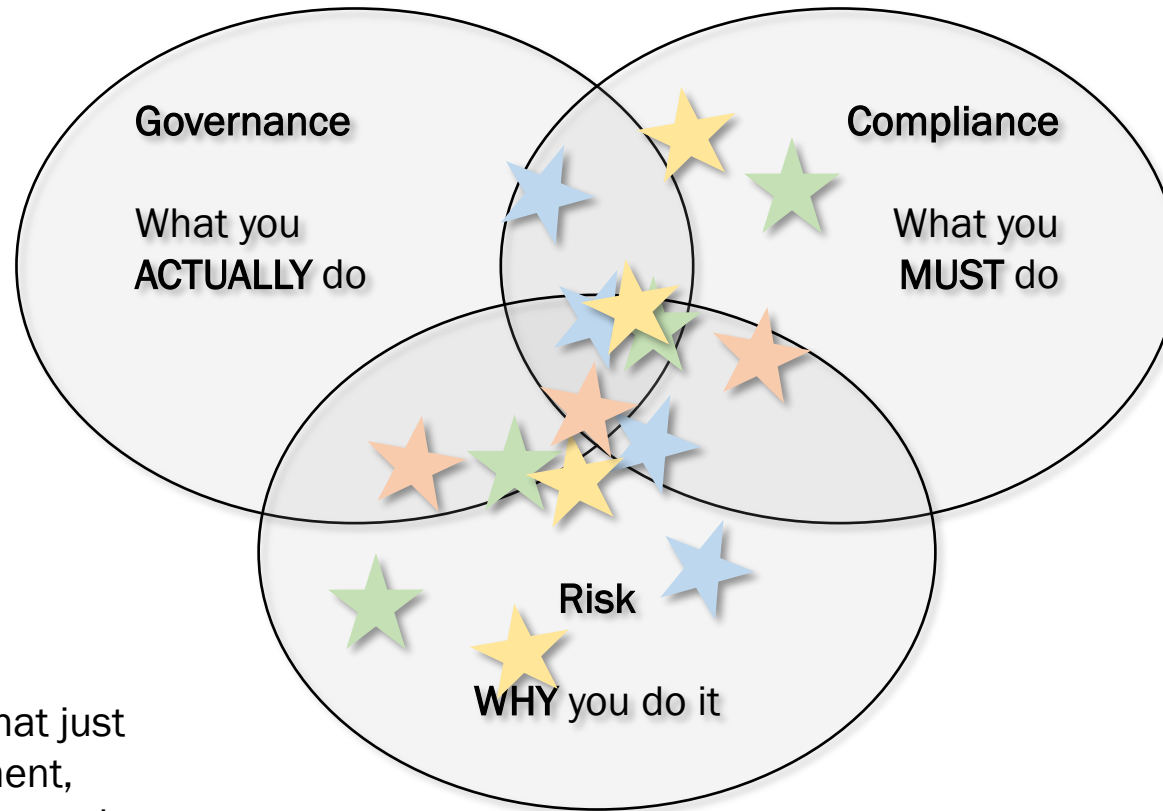












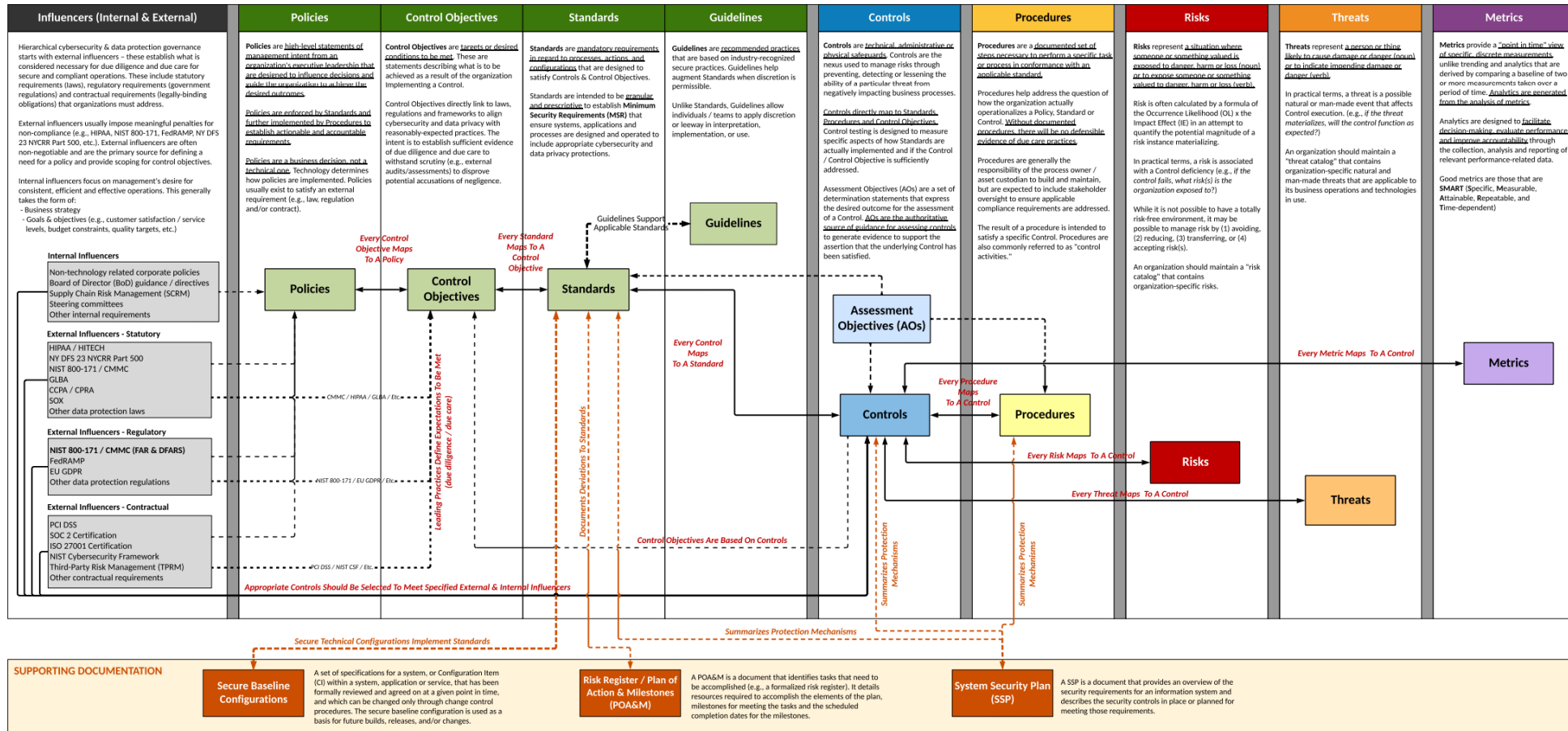
Some random group that just bypassed procurement, bought new equipment and software, and is mining Bitcoin to fund their projects

**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 (internal and external).

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

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

## Top-Down Process Flow of Cybersecurity & Privacy Governance Concepts

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 requirements are enforced.

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?).

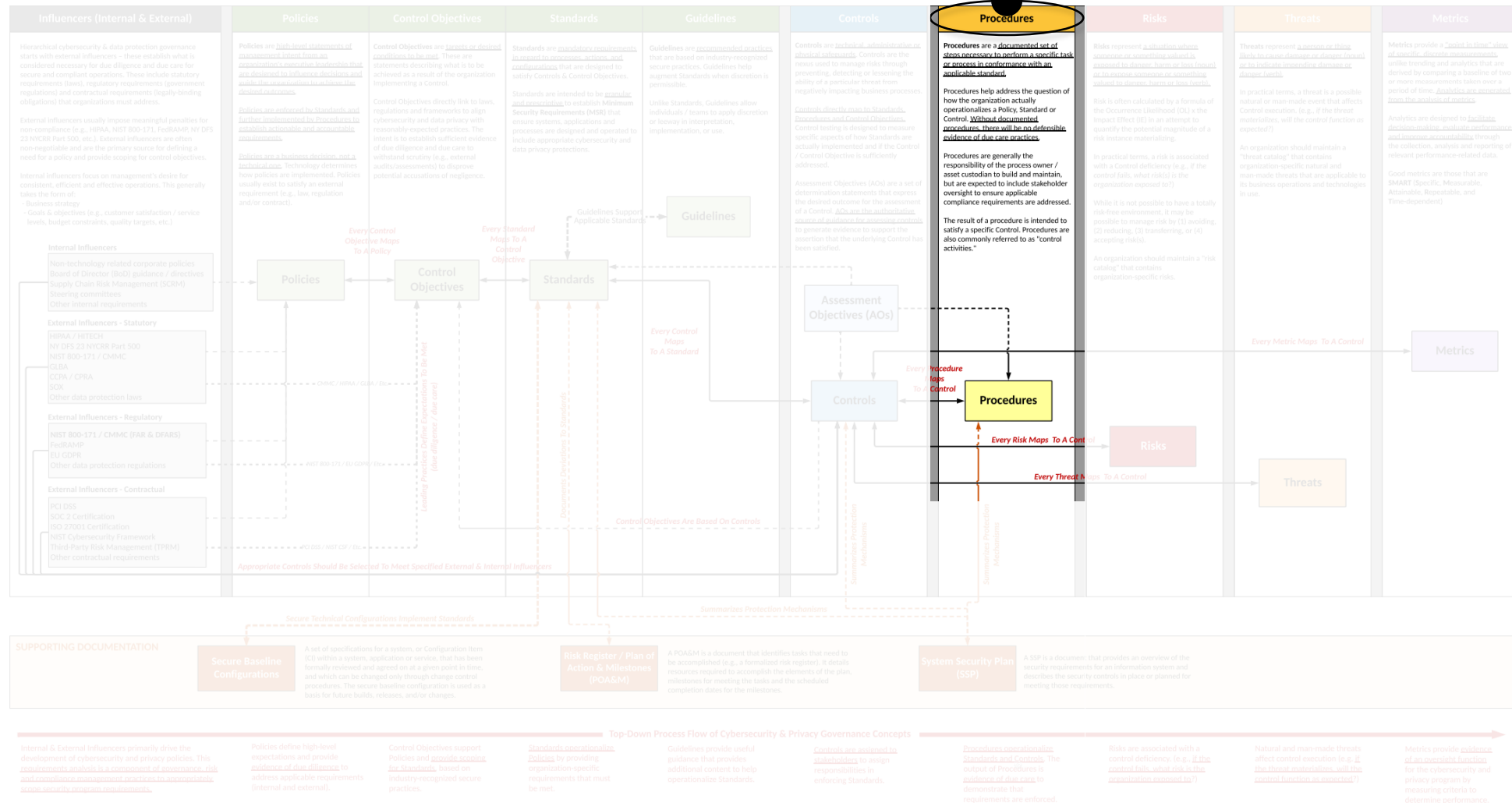
Metrics provide evidence of an oversight function for the cybersecurity and privacy program by measuring criteria to determine performance.

# How do we actually succeed then?

ALWAYS LEADING



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

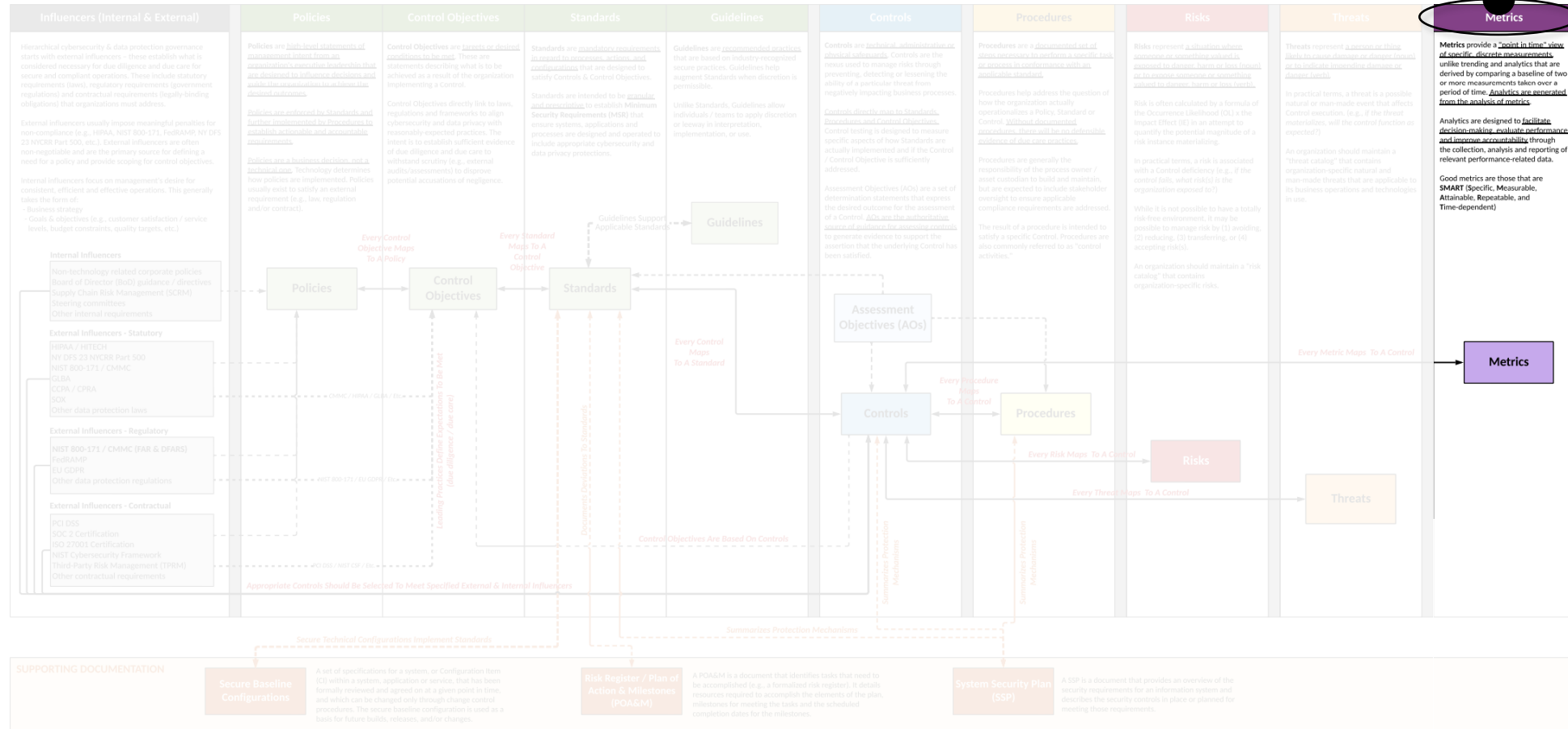


# How do we actually succeed then?

ALWAYS LEADING



Sometimes you'll even be doing this...



Internal & External Influencers primarily drive the development of cybersecurity and privacy policies. This development analysis is a component of governance, risk and compliance management necessary to representative appropriate 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 for Standards, based on industry-recognized secure practices.

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.

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

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?)

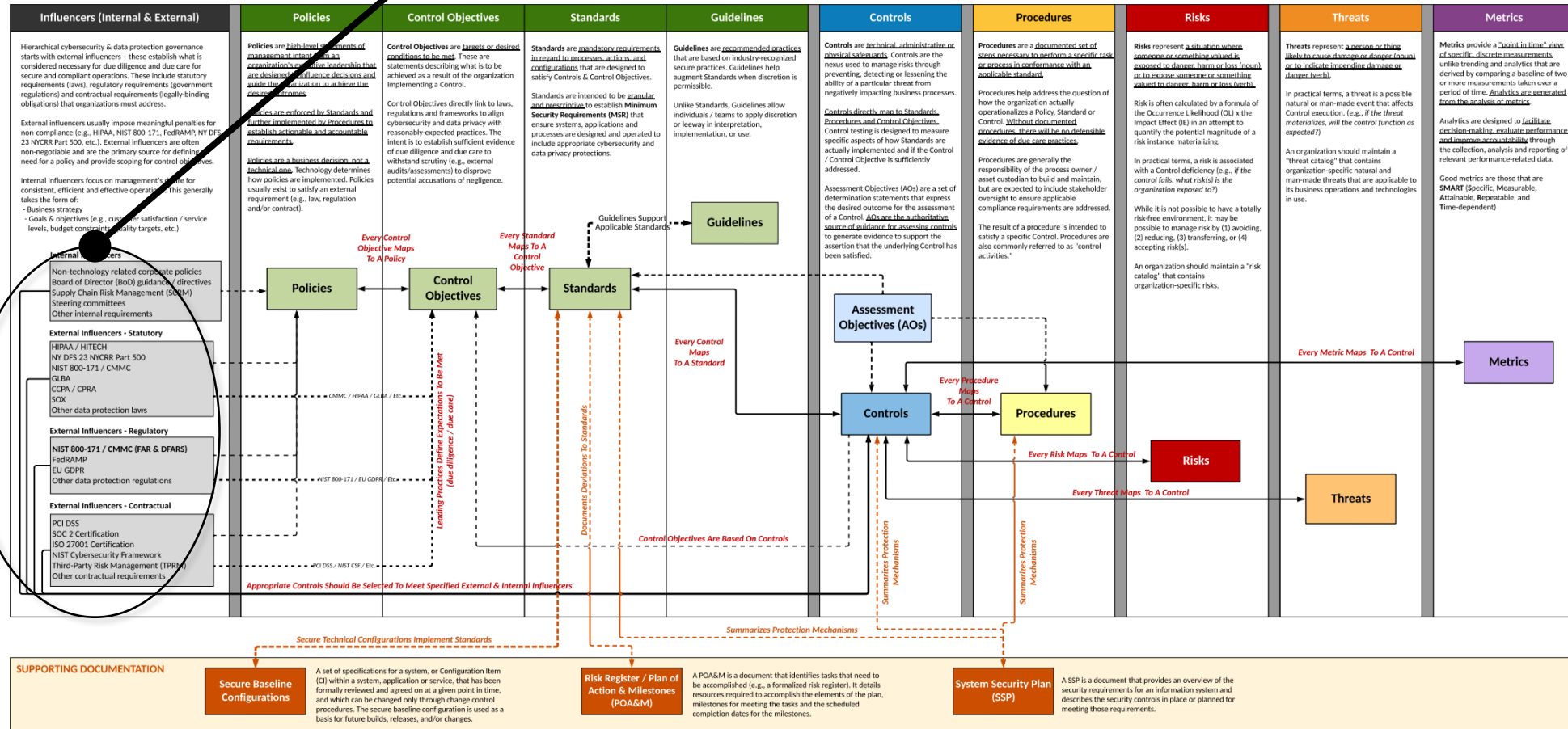
Metrics provide guidance of an oversight function for the cybersecurity and privacy program by measuring criteria to determine performance.





**COMPLIANCE  
FORGE**

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 (internal and external).

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

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

## Top-Down Process Flow of Cybersecurity & Privacy Governance Concepts

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 requirements are enforced.

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

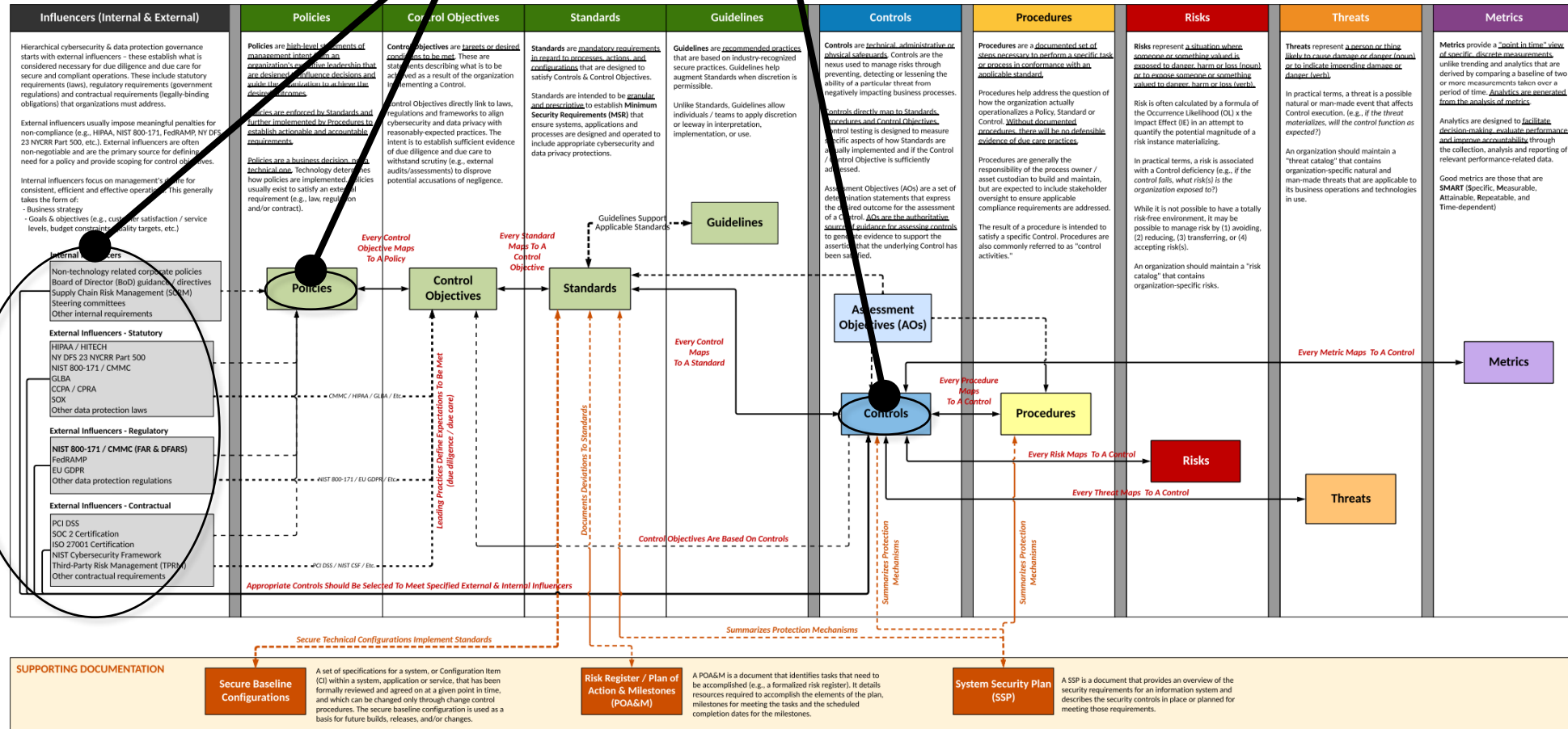
Natural and man-made threats affect control execution (e.g., if the threat materializes, will the control function as expected?).

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



## COMPLIANCE FORGE

## 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 (internal and external).

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

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

### Top-Down Process Flow of Cybersecurity & Privacy Governance Concepts

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 requirements are enforced.

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 evidence of an oversight function for the cybersecurity and privacy program by measuring criteria to determine performance.

## ALWAYS LEADING



**Cybersecurity Framework**

Influencers (Internal & External)	Policies	Control Objectives	Standards	Guidelines	Controls	Procedures	Risks	Threats	Metrics
<b>Hierarchical cybersecurity &amp; data protection governance</b> starts with external influencers – these establish what is considered necessary for due diligence and due care for secure and compliant operations. These include statutory requirements (laws), regulatory requirements (government regulations) and contractual requirements (legally-binding obligations) that organizations must address.  <b>External influencers</b> usually impose meaningful penalties for non-compliance (e.g., HIPAA, NIST 800-171, FedRAMP, NY DFS 23 NYCRR Part 500, etc.). External influencers are often non-negotiable and are the primary source for defining need for a policy and provide scoping for control objectives.  <b>Internal influencers</b> focus on management's desire for consistent, efficient and effective operation. This generally takes the form of: - Business strategy - Goals & objectives (e.g., customer satisfaction / service levels, budget constraints, quality targets, etc.)  <b>Internal Influencers</b> Non-technology related corporate policies Board of Director (BoD) guidance / directives Supply Chain Risk Management (SCRM) Steering committees Other internal requirements  <b>External Influencers - Statutory</b> HIPAA / HITECH NY DFS 23 NYCRR Part 500 NIST 800-171 / CMMC GLBA CCPA / CPRA SOX Other data protection laws  <b>External Influencers - Regulatory</b> NIST 800-171 / CMMC (FAR & DFARS) FedRAMP EU GDPR Other data protection regulations  <b>External Influencers - Contractual</b> PCI DSS SOC 2 Certification ISO 27001 Certification NIST Cybersecurity Framework Third-Party Risk Management (TPRM) Other contractual requirements	<b>Policies</b> are high-level statements of management intent. They are organizational-level decisions that are designed to guide decision-making and establish the foundation for all other cybersecurity measures.  <b>Policies</b> are enforced by Standards and further implemented by Procedures to establish actionable and measurable requirements.  <b>Policies</b> are a business decision. Technology determines how policies are implemented. Policies usually exist to satisfy an external requirement (e.g., law, regulation and/or contract).	<b>Control Objectives</b> are targets or desired conditions to be met. These are statements describing what is to be achieved as a result of the organization implementing a Control.  <b>Control Objectives</b> directly link to laws, regulations and frameworks to align cybersecurity and data privacy with reasonably expected practices. The intent is to establish sufficient evidence of due diligence and due care to withstand scrutiny (e.g., external audits/assessments) to disprove potential accusations of negligence.	<b>Standards</b> are mandatory requirements intended to establish Minimum Security Requirements (MSR) that ensure systems, applications and processes are designed and operated to include appropriate cybersecurity and data privacy protections.	<b>Guidelines</b> are recommended practices that are based on industry-recognized secure practices. Guidelines help augment Standards when discretion is permissible.  Unlike Standards, Guidelines allow individuals / teams to apply discretion or leeway in interpretation, implementation, or use.	<b>Controls</b> are technical, administrative or physical safeguards. Controls are the means used to manage risks through preventing, detecting or lessening the ability of a particular threat from negatively impacting business processes.  <b>Controls</b> directly map to Standards, Procedures and Control Objectives.  <b>Assessment Objectives (AOs)</b> are a set of determination statements that express the desired outcome for the assessment of a Control. AOs are the authoritative source of guidance for assessing controls to generate evidence to support the assertion that the underlying Control has been satisfied.	<b>Procedures</b> are a documented set of steps necessary to perform a specific task or process in conformance with an applicable standard.  <b>Procedures</b> help address the question of how the organization actually operationalizes a Policy, Standard or Control. Without documented procedures, there will be no defensible evidence of due-care practices.  <b>Procedures</b> are generally the responsibility of the process owner / asset custodian to build and maintain, but are expected to include stakeholder oversight to ensure applicable compliance requirements are addressed.  The result of a procedure is intended to satisfy a specific Control. Procedures are also commonly referred to as "control activities."	<b>Risks</b> represent a situation where an adverse event may occur, resulting in harm or loss (reputational, financial, operational, legal, etc.) to an organization.  <b>Risks</b> are calculated by a formula of the Occurrence Likelihood (OL) x the Impact Effect (IE) in an attempt to quantify the potential magnitude of a risk scenario.  In practical terms, a risk associated with a Control deficiency exists if, if the controls fail, what risk(s) does the organization exposed to?  While it is not possible to have a totally risk-free environment, it may be possible to manage risk by (1) avoiding, (2) reducing, (3) transferring, or (4) accepting risk(s).  An organization should maintain a "risk catalog" that contains organization-specific risks.	<b>Threats</b> represent a person or thing likely to cause damage or danger (personnel, system, technology, etc.) to an organization.  In practical terms, a threat is a possible natural or man-made event that affects Control execution. (e.g., if the threat materializes, will the control function as expected?)  An organization should maintain a "threat catalog" that contains organization-specific natural and man-made threats that are applicable to its business operations and technologies in use.	<b>Metrics</b> provide a "point in time" view of security-related measurements unlike trending and analytics that are derived by comparing a baseline of two or more measurements taken over a period of time. Analytics are generated from the analysis of metrics.  <b>Analytics</b> are designed to facilitate decision-making, evaluate performance and improve accountability through the collection, analysis and reporting of relevant performance-related data.  Good metrics are those that are SMART (Specific, Measurable, Attainable, Repeatable, and Time-dependent)

**SUPPORTING DOCUMENTATION**

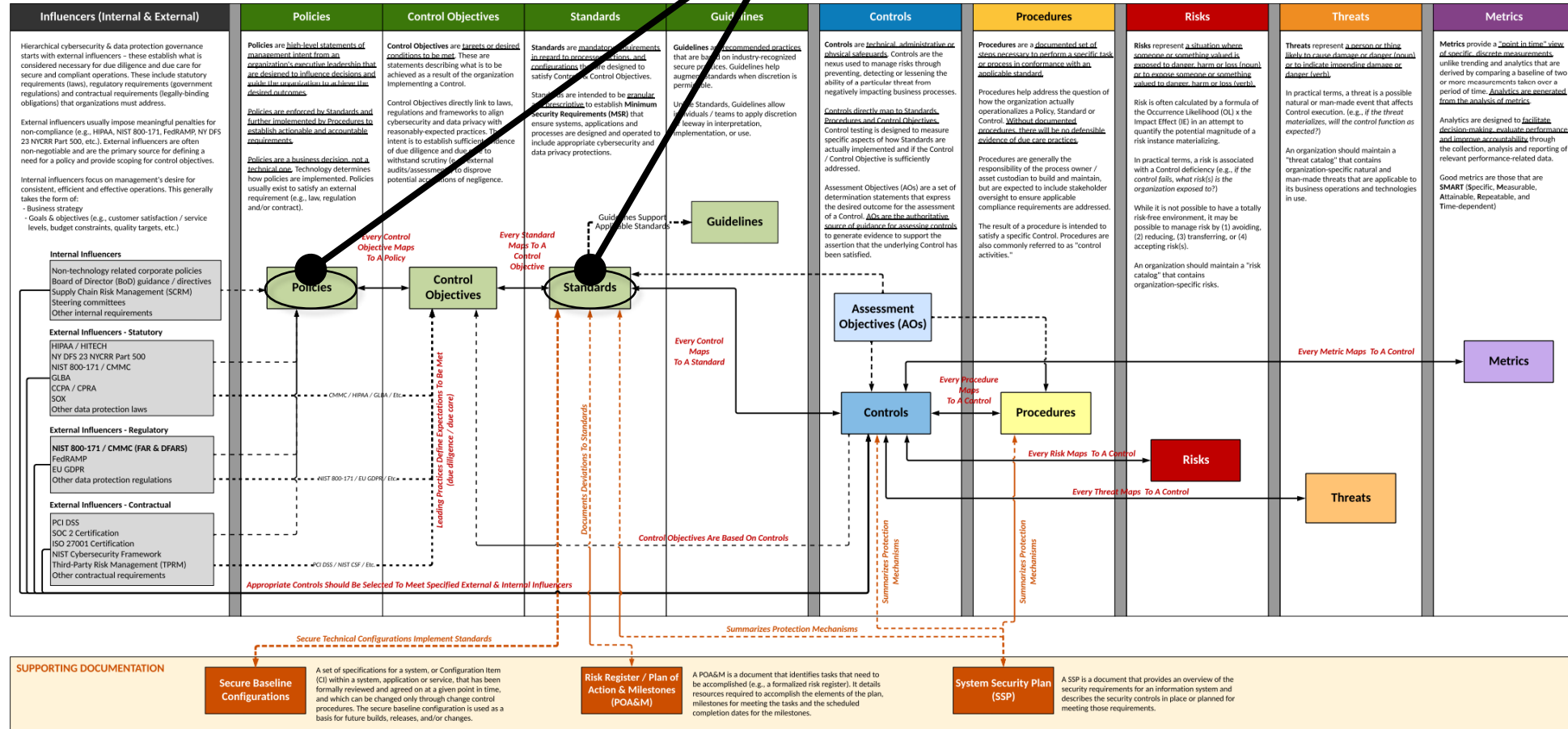
- Secure Baseline Configurations:** A set of specifications for a system, or Configuration Item (CI) within a system, application or service, that are formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The secure baseline configuration is used as a basis for future builds, releases, and/or changes.
- Risk Register / Plan of Action & Milestones (POA&M):** A POA&M is a document that identifies tasks that need to be accomplished (e.g., a formalized risk register). It details resources required to accomplish the elements of the plan, milestones for meeting the tasks and the scheduled completion dates for the milestones.
- System Security Plan (SSP):** A SSP is a document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

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





## Technical Standards VS Risk Management Standards



**Top-Down Process Flow of Cybersecurity & Privacy Governance Concepts**

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 (internal and external).

Control Objectives support Policies and provide scoping for Standards, based on industry-recognized security practices.

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.

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

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 evidence of an oversight function for the cybersecurity and privacy program by measuring criteria to determine performance.

Is it really PowerShell though?

ALWAYS LEADING





- **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)



- **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)



- **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 (ESAE, 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 (ESAE, 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 (ESAE, 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 (ESAE, 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@sentinel.com](mailto:misoule@sentinel.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

