

# Cybersecurity Best Practices: US Government Perspective

**Tyson Scott – Consulting Systems Engineer**

**US Public Sector Cybersecurity**

February 2014



# Background

# Cybersecurity in the US Government

Making it work

## Central Agency for Cybersecurity



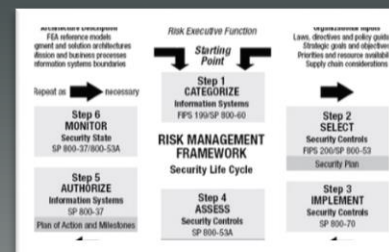
US Department of Homeland Security  
National Protection and Programs Directorate

## Standards Organizations



National Institute for Standards and Technology  
The MITRE Corporation

## Best Practices and Frameworks



800 Series Publications  
Cybersecurity Framework  
Risk Management Framework

## Acceleration Programs



C<sup>3</sup> Voluntary Program  
FedRAMP  
Continuous Diagnostics and Mitigation Program

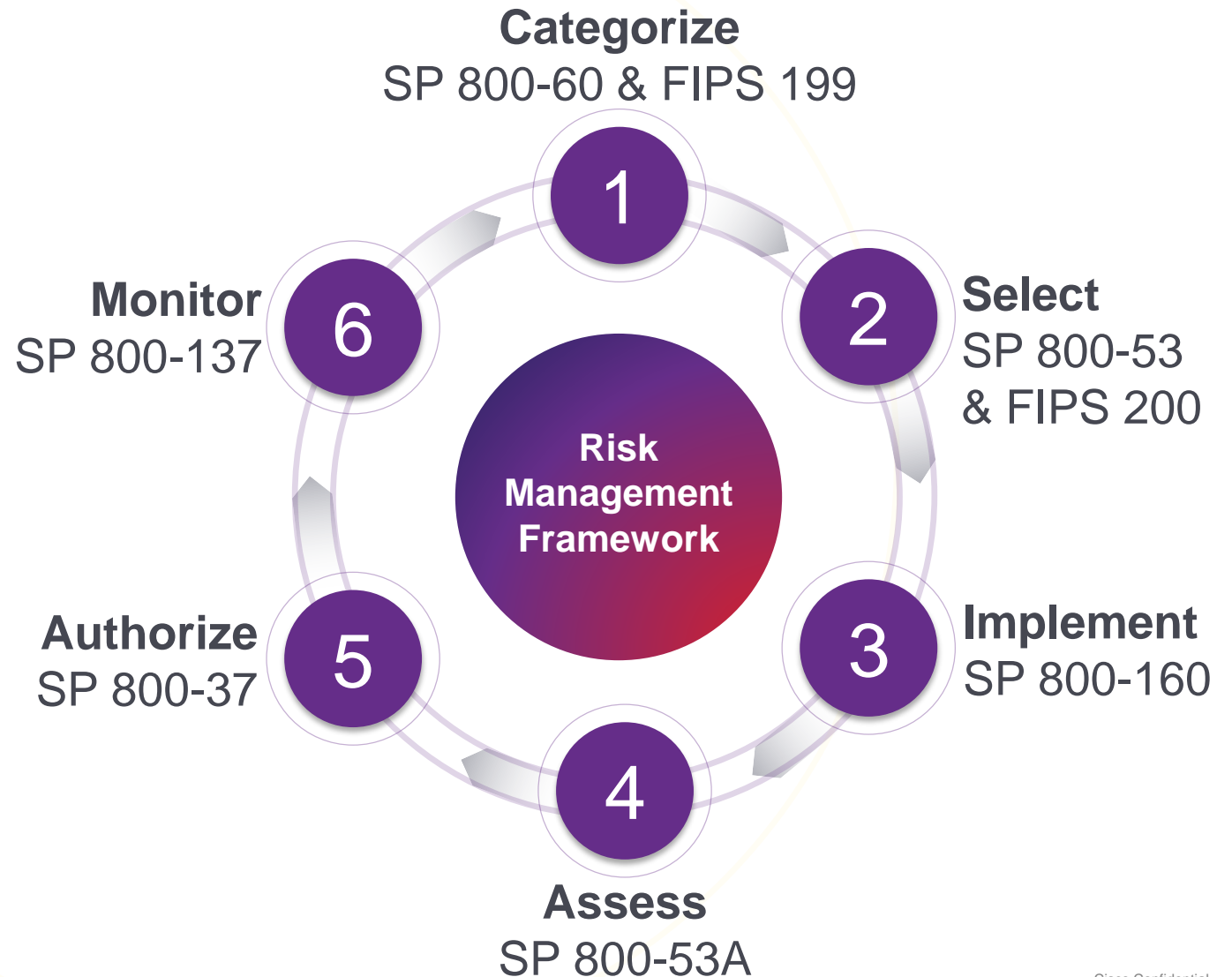
Cybersecurity  
Legislation

# NIST Risk Management Framework (RMF)

## Security Life Cycle



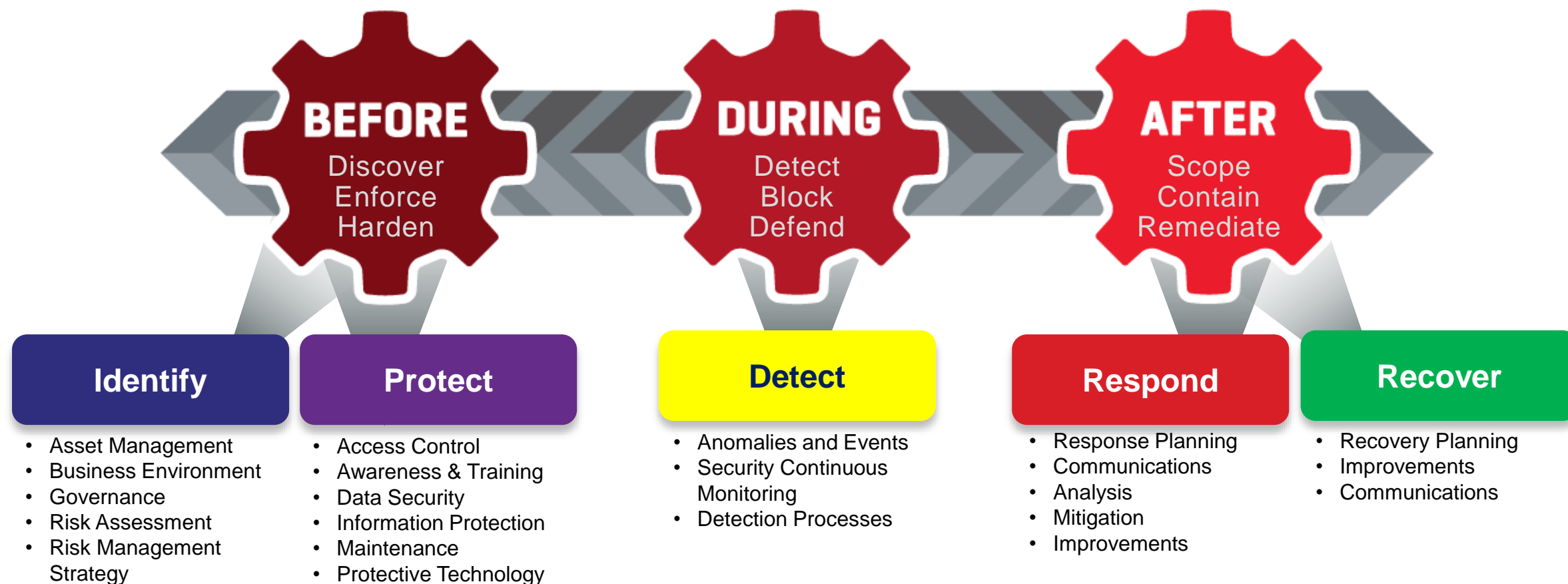
The RMF pulls it all together into an **information security continuous monitoring** process



# Cisco Security and the Cybersecurity Best Practices




# The Threat-Centric Security Model

## Aligning with the Cybersecurity Framework Core


























































# The Threat-Centric Security Model

## Aligning with the CDM Program

-  Covers Full Control Model
-  Covers Part of Control Model
-  With ISE PxGrid and a 3<sup>rd</sup> Party

Aligning with the CDM Program

CDM Phase			Tool Functional Areas ("CDM Tools")										ISE/TrustSec	Meraki SME	ASA/FP Services	Next-Gen IPS	FireSIGHT	AMP	ESA	WSA	Anyconnect	Lancope
1	1	Hardware Asset Management																				
	2	Software Asset Management																				
	3	Configuration Settings Management																				
	4	Vulnerability Management																				
2	5	Manage Network Access Controls																				
	6	Manage Trust in People Granted Access																				
	7	Manage Security-Related Behavior																				
	8	Manage Credentials and Authentication																				
	9	Manage Account Access/Manage Privileges																				
3	10	Prepare for Contingencies and Incidents																				
	11	Respond to Contingencies and Incidents																				
	12	Design/Build-In Requirements Policy/Planning																				
	13	Design/Build-In Quality																				
	14	Manage Audit Information																				
	15	Manage Operation Security																				

Confidential7

# Closing Remarks



# Security Manifesto for today's world

- **Security** must support the business
- **Security** must work with existing architecture—and be usable
- **Security** must be transparent and informative
- **Security** must enable visibility and appropriate action
- **Security** must be viewed as a “people problem”



Cisco Annual Security Report 2015

Thank You

