HACKTOBER 2022

WaTech
Washington Technology Solutions

# From Compliance to Risk-Awareness

A Security Agility Journey

Stevens F. Fox
Deputy CISO for Policy and Program Management

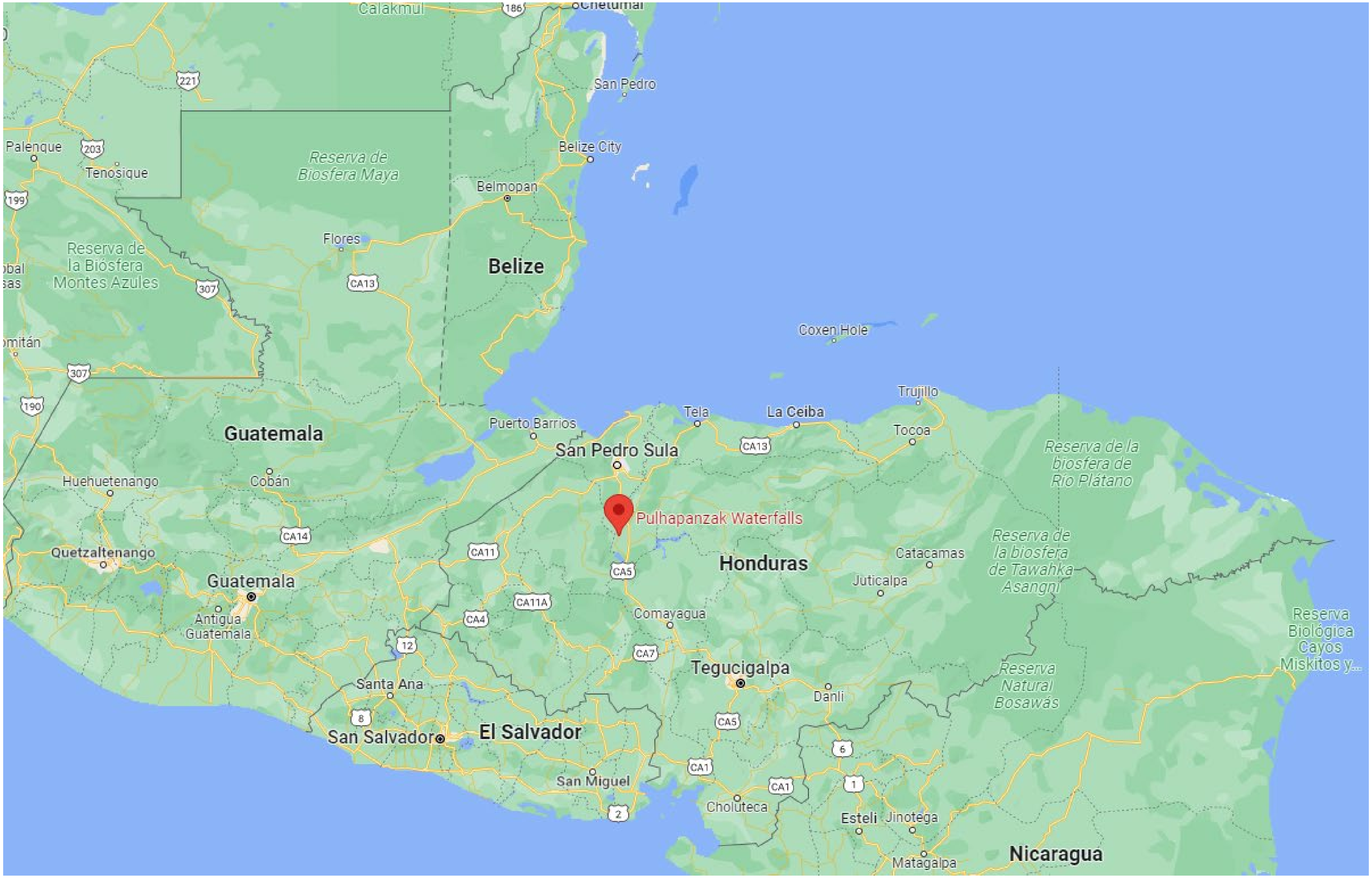
## Agenda

- Case Study – Mission Pulhapanzak
- Program framework
- Call to Action
- Q/A

Information Security is about Risk Management

# Requirements for a risk-aware agency community

- Risk ownership.
- Uniform framework.
- Risk-focus.
- Compliance as a baseline.


Calakmul
186
Chetumal
221
San Pedro
Palenque
203
Tenosique
Reserva de
Biosfera Maya
Belize City
199
Belmopan
Flores
Reserva de
la Biósfera
Montes Azules
bal
sas
307
CA13
Belize
Coxen Hole
mitán
307
190
Trujillo
Tela
La Ceiba
Puerto Barrios
Tocoa
Guatemala
San Pedro Sula
CA13
Reserva de la
biosfera de
Río Plátano
Huehuetenango
Cobán
Pulhapanzak Waterfalls
CA14
Quetzaltenango
CA11
Reserva de
la biosfera
de Tawahka
Asangni
Catacamas
Honduras
CA5
Guatemala
Juticalpa
CA11A
Antigua
Guatemala
CA4
Comayagua
Reserva
Biológica
Cayos
Miskitos y...
12
CA7
Tegucigalpa
Reserva
Natural
Bosawás
Santa Ana
Danlí
8
CA5
San Salvador
El Salvador
6
CA1
San Miguel
CA1
1
2
Choluteca
Estelí
Jinotega
Matagalpa
Nicaragua

# Mission Pulhapanzak: Reach the Waterfall Base

# Why would I do this?

# Hazard Recognition

# Threats

- Jagged gorge walls
- Boulder-laden rapids
- Waterfall hydraulics

Uneven, wet ledges

Underwater logs

Falling debris

## Vulnerabilities

- Blunt & Sharp Force Trauma
- Lack of experience
- Disorientation

# Waterfall Safety Tips

1. Wear sturdy hiking shoes or boots.

2. Stay on developed trails.

3. Pay attention to warning signs and rules posted near waterfalls.

4. Never climb on or around waterfalls.

5. Never jump off waterfalls or dive into plunge pools.

6. Supervise children and pets carefully.

7. Never play in the stream or river above a waterfall, or try to take photos at the top of a waterfall.

WaTech
Washington Technology Solutions

# Is this enough information?

JACK DANI
Old
NO.
Tenn

# Intel from my team

- October – February is the high-hazard window.
  - Ideal time between March and June
- Sections of the waterfall to avoid.
- Circumstances behind injuries and deaths.

# Tips from my team

- Safety vs. Maneuverability.
- Focus on footing, balance, and grip.
- Carelessness leads to injury or worse.

# Focus through Context

# The Risks

shutterstock.com · 289455668

# Preparation

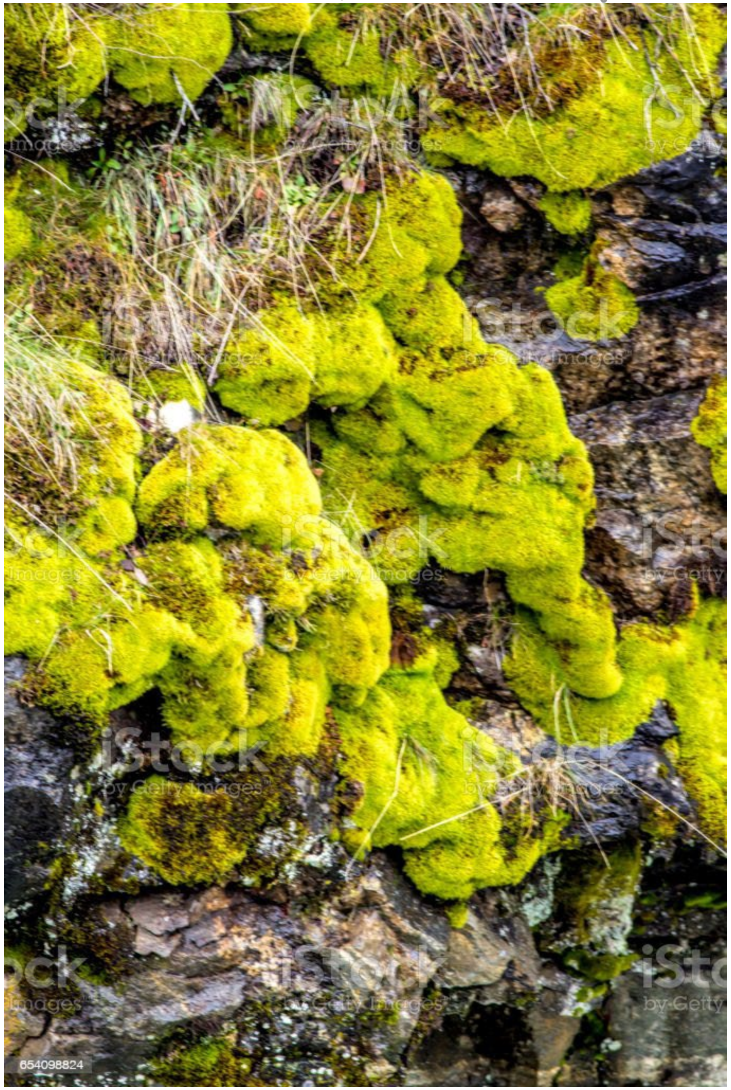
- Physical and mental training.

- Purchase safety gear.
  - Water shoes
  - Flotation vest
  - Head gear

# The Day of Truth

# Key Risk Indicators

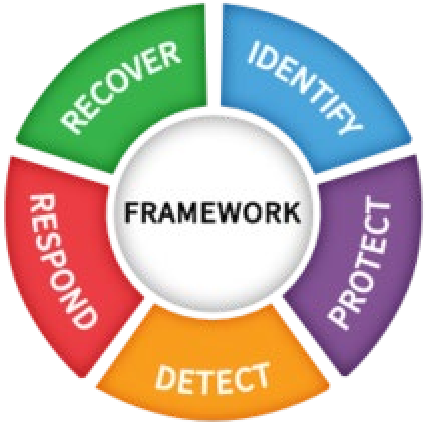
- Poor weather conditions.
- Unstable cliff walls.
- Presence of dangerous animals.

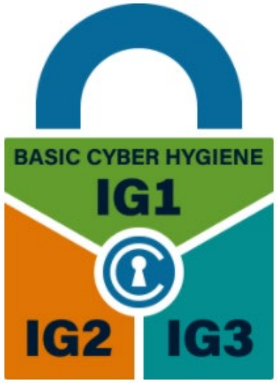


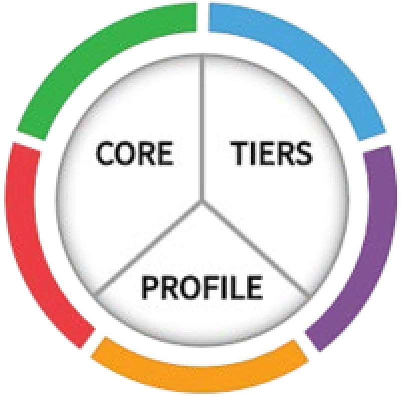
# Applying these lessons to your agency

# Risk Team

- Threats – Verizon threat report, Security Operations, US-CERT, threat intel.
- Vulnerabilities – Security Operations, vulnerability intel, CISA.
- Business Impact – Agency management and Enterprise Security Governance







**Program**

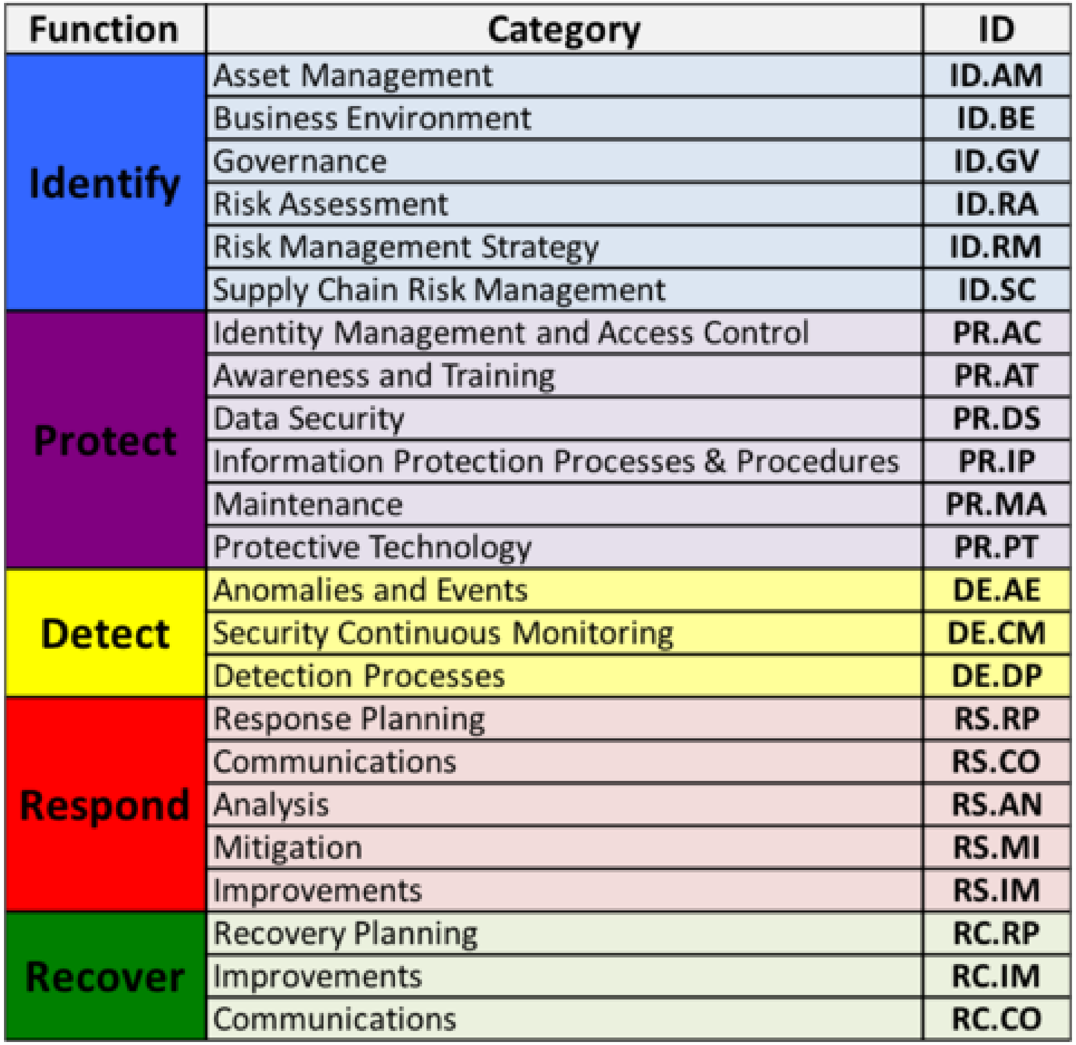
**Control**

**Risk Management**

# CSF Core – Strategy Level

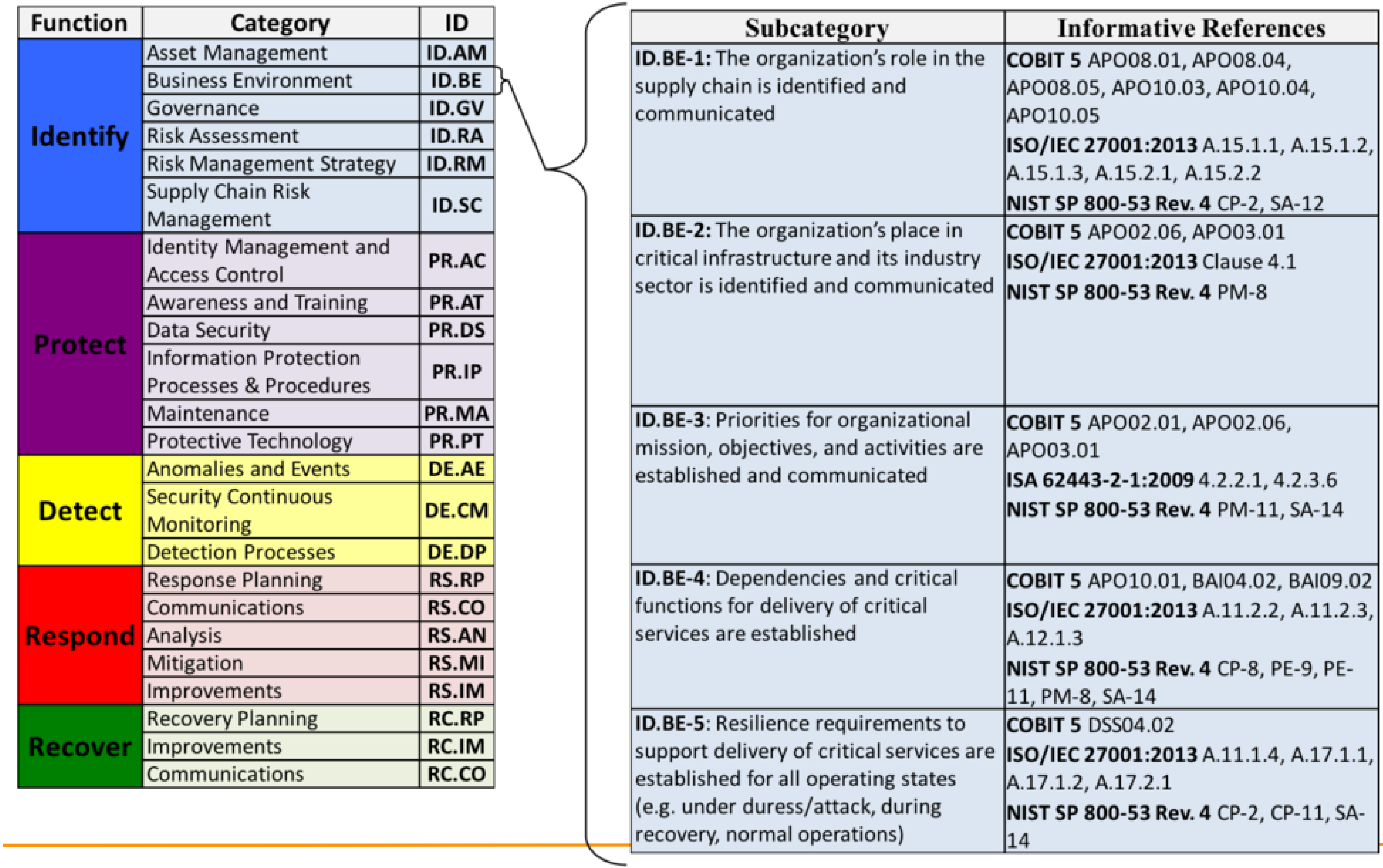
| Function | Objective |
|---|---|
| Identify | Identify risks to systems and data. |
| Protect | Safeguard the delivery of agency capabilities. |
| Detect | Detection of cybersecurity events that pose a threat. |
| Respond | Respond to mitigate the impact of a cybersecurity event. |
| Recover | Restore capabilities impaired due to a cybersecurity event. |

# CSF Core – Tactical Level



| Function | Category | ID |
|---|---|---|
| Identify | Asset Management | ID.AM |
| | Business Environment | ID.BE |
| | Governance | ID.GV |
| | Risk Assessment | ID.RA |
| | Risk Management Strategy | ID.RM |
| | Supply Chain Risk Management | ID.SC |
| Protect | Identity Management and Access Control | PR.AC |
| | Awareness and Training | PR.AT |
| | Data Security | PR.DS |
| | Information Protection Processes & Procedures | PR.IP |
| | Maintenance | PR.MA |
| | Protective Technology | PR.PT |
| Detect | Anomalies and Events | DE.AE |
| | Security Continuous Monitoring | DE.CM |
| | Detection Processes | DE.DP |
| Respond | Response Planning | RS.RP |
| | Communications | RS.CO |
| | Analysis | RS.AN |
| | Mitigation | RS.MI |
| | Improvements | RS.IM |
| Recover | Recovery Planning | RC.RP |
| | Improvements | RC.IM |
| | Communications | RC.CO |

# CSF Core – Operational Level

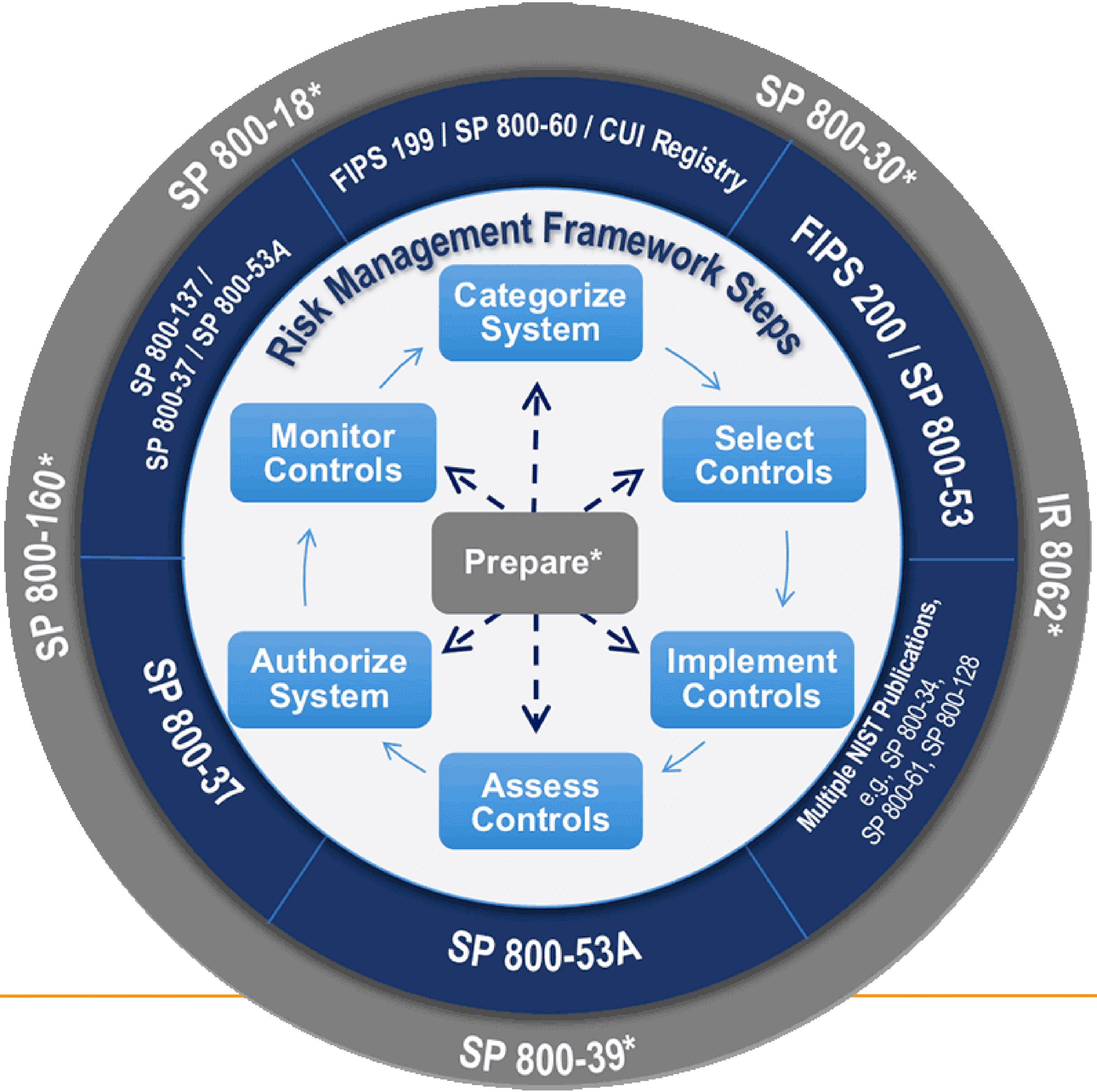


| Function | Category | ID |
|---|---|---|
| Identify | Asset Management | ID.AM |
| | Business Environment | ID.BE |
| | Governance | ID.GV |
| | Risk Assessment | ID.RA |
| | Risk Management Strategy | ID.RM |
| | Supply Chain Risk Management | ID.SC |
| Protect | Identity Management and Access Control | PR.AC |
| | Awareness and Training | PR.AT |
| | Data Security | PR.DS |
| | Information Protection Processes & Procedures | PR.IP |
| | Maintenance | PR.MA |
| | Protective Technology | PR.PT |
| Detect | Anomalies and Events | DE.AE |
| | Security Continuous Monitoring | DE.CM |
| | Detection Processes | DE.DP |
| Respond | Response Planning | RS.RP |
| | Communications | RS.CO |
| | Analysis | RS.AN |
| | Mitigation | RS.MI |
| | Improvements | RS.IM |
| Recover | Recovery Planning | RC.RP |
| | Improvements | RC.IM |
| | Communications | RC.CO |

| Subcategory | Informative References |
|---|---|
| **ID.BE-1:** The organization's role in the supply chain is identified and communicated | **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05<br>**ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2<br>**NIST SP 800-53 Rev. 4** CP-2, SA-12 |
| **ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated | **COBIT 5** APO02.06, APO03.01<br>**ISO/IEC 27001:2013** Clause 4.1<br>**NIST SP 800-53 Rev. 4** PM-8 |
| **ID.BE-3**: Priorities for organizational mission, objectives, and activities are established and communicated | **COBIT 5** APO02.01, APO02.06, APO03.01<br>**ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6<br>**NIST SP 800-53 Rev. 4** PM-11, SA-14 |
| **ID.BE-4**: Dependencies and critical functions for delivery of critical services are established | **COBIT 5** APO10.01, BAI04.02, BAI09.02<br>**ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3<br>**NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14 |
| **ID.BE-5**: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) | **COBIT 5** DSS04.02<br>**ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1<br>**NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14 |

# CSF Tiers

| Focus Area | Tier 1 - Partial | Tier 2 - Risk Informed | Tiers 3 - Repeatable | Tier 4 - Adaptive |
|---|---|---|---|---|
| People | Little awareness of agency risk. | An agency is aware of its risk. However, implementation of cybersecurity measures to manage risk is piecemeal. | Agency implements policy and procedures to manage risk consistently. | Agency anticipates risk management needs by analyzing internal and external trends. The agency also collaborates with other agencies with common missions to manage risk at the State level. |
| Process | | | | |
| Technology | | | | |
| State | | Target Tier | | |


Risk Management Framework Steps
Categorize System
Select Controls
Implement Controls
Assess Controls
Authorize System
Monitor Controls
Prepare*
FIPS 199 / SP 800-60 / CUI Registry
FIPS 200 / SP 800-53
Multiple NIST Publications, e.g., SP 800-34, SP 800-61, SP 800-128
SP 800-53A
SP 800-37
SP 800-137 / SP 800-37 / SP 800-53A
SP 800-18*
SP 800-30*
IR 8062*
SP 800-39*
SP 800-160*

# Risk Monitoring

## Risk Indicators

- Derived from a risk assessment.
- Lagging indicators alert to risks that happened.
- Leading indicators are an early-warning system.C

## Control Indicators

- Derived from a risk assessment.

## Types

- Internal audits.
- Vulnerability scans.
- Penetration tests

# Call to action

- Identify your risk team.
- Understand the org risk management maturity level.
- Make the risk tangible.

# Questions?