



The NIST Framework High Value for ITS

Shannon Barnes, CIO

Craig Schumacher, CISO

Idaho Transportation Department

September 2015



NIST Cybersecurity Framework

- National Institute of Standards (nist.gov)
- Published in February 2014 - a collection of standards, guidelines and practices for reducing cyber risks to critical infrastructure
- Industry and private sector partnership
- Website <http://www.nist.gov/cyberframework>



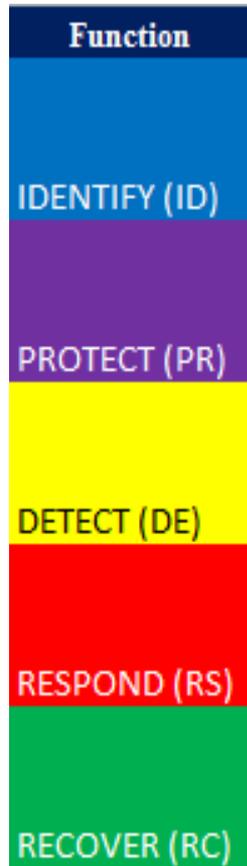
Why use NIST Framework

- Helps to better understand, manage, and reduce cybersecurity risks.
- Determine which activities are most important to assure critical operations and service delivery.
- Prioritize investments and maximize the impact of each dollar spent on cybersecurity.
- Show executives in a objective quantitative manner the status of the program and where improvements are needed.



NIST Framework Details

Functions organize basic cybersecurity activities at their highest level

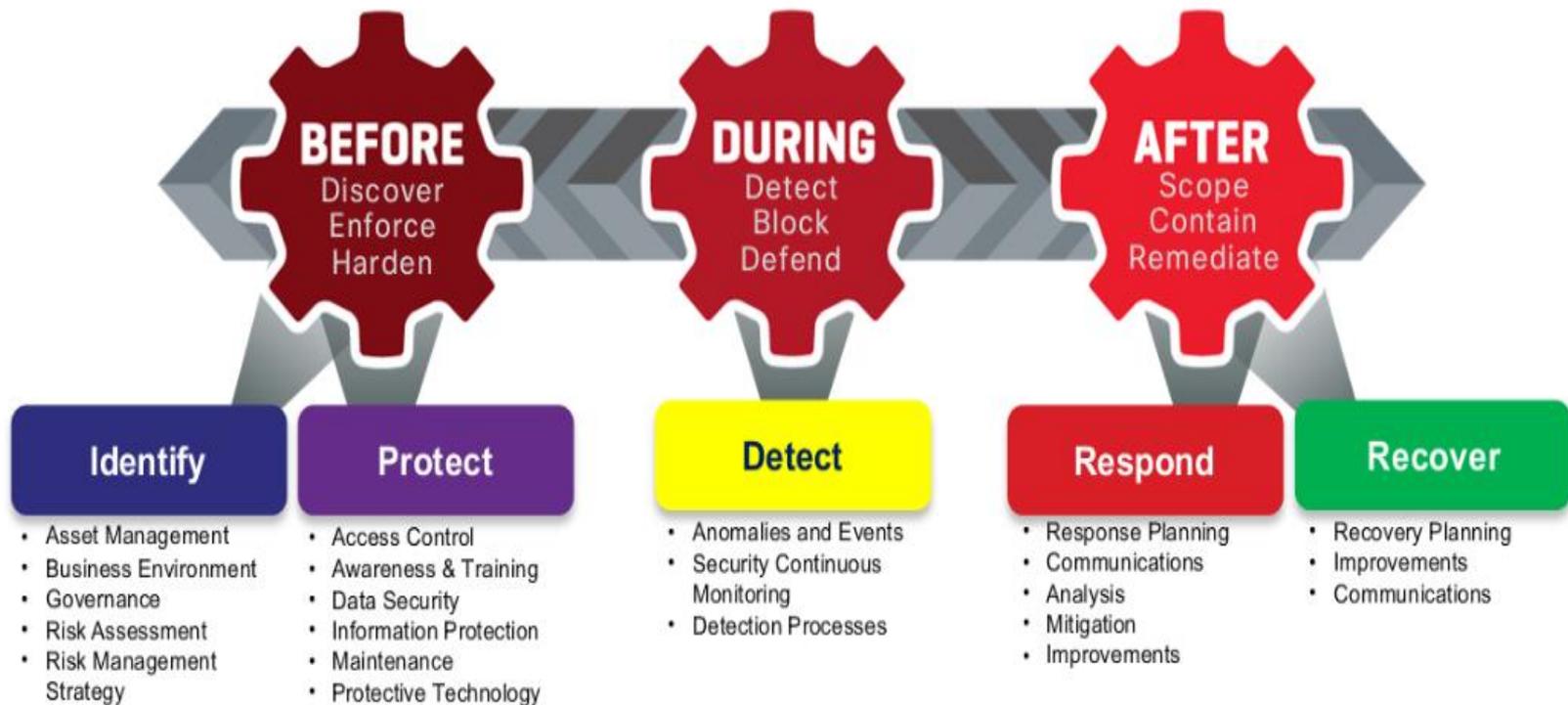


- **Identify, Protect, Detect, Respond, and Recover**
- Functions aid ITD in managing risk by:
 - Organizing information
 - Enabling risk management decisions
 - Addressing threats
 - Show the impact of investments in cybersecurity.

Putting the Functions in Perspective

The Threat-Centric Security Model

Aligning with the Cybersecurity Framework Core





NIST Framework Details

■ Functions

- **Categories** - groups of cybersecurity outcomes closely tied to programmatic needs
 - **Subcategories** - specific outcomes of technical and/or management activities
 - **Controls**- illustrate a method to achieve the outcomes

■ Rated by Tiers

Tier Score	Tier
0	Nothing
1	Partial
2	Risk Informed (Communicated)
3	Repeatable
4	Adaptive

How did we measure our progress



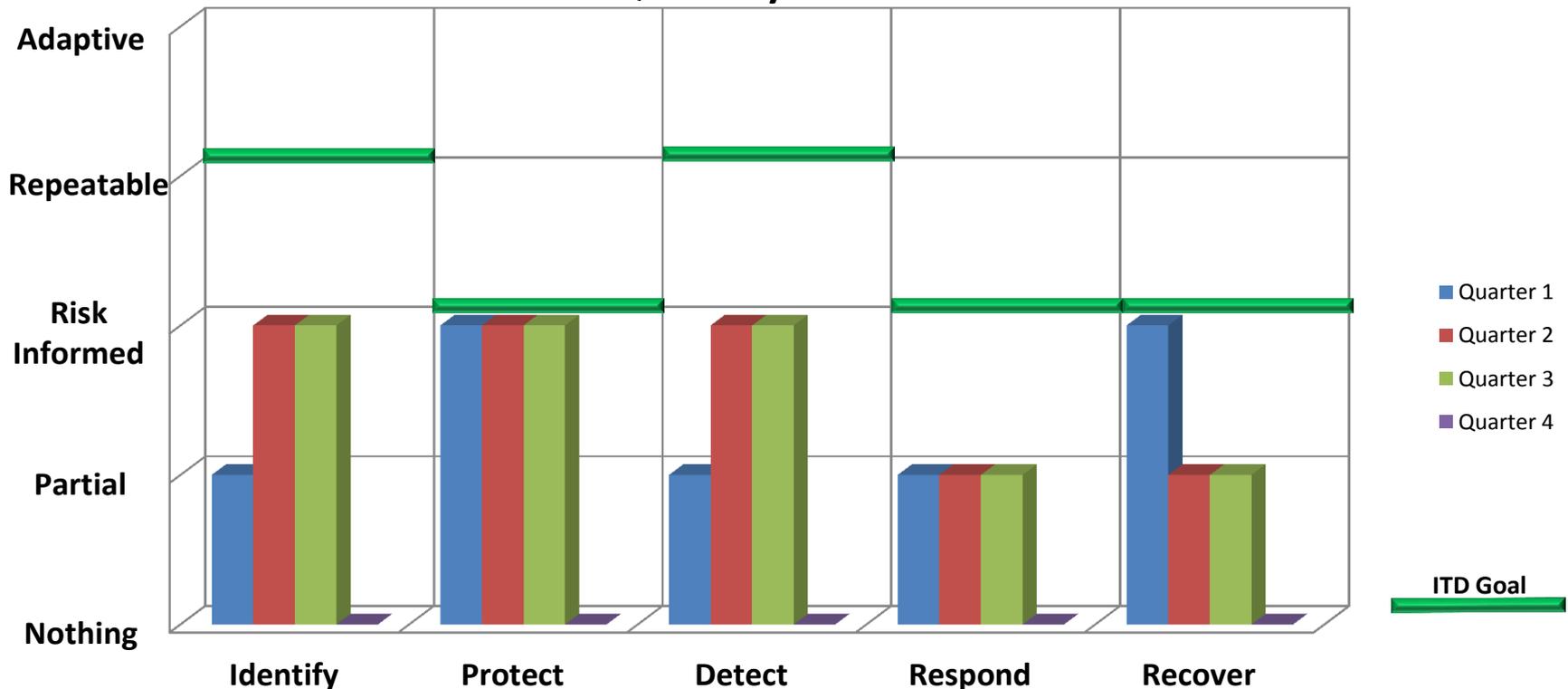
- Developed a matrix (Excel spreadsheet) to evaluate the framework by Sub Category by Tier
- Baselined (took an informed guess) at where we were on the framework
- Set (aggressive) goals on where we think we should be in 3 to 5 years
- Created a method of scoring the NIST by numeric value of the Tier (0 through 4) by Sub Category.



Visual Management – Key to Success

Create a baseline, set goals, evaluate progress routinely and communicate progress and risks

ITD NIST Cyber Security Functions and Goals
Quarterly - FY 2015





Lessons Learned

- Team was focused on improving areas we were already strong in, not on the things we were weak.
- Our baseline was fairly optimistic.
- Some scores dropped because we gained a better understanding of what was needed and what we were doing.

ITS Opportunities

- **Identify** ID.RA-1
- **Protect** PR.AC-1, PR.AC-2, PR.AC-3, PR.AC-5, PR.AT-3, PR.DS-3, PR.IP-3, PR.MA-1, PR.MA-2, PR.PT-3, PR.PT-4
- **Detect** DE.AE-2, DE.AE-2, DE.CM-2, DE.CM-7, DE.CM-8, DE.DP-2, DE.DP-3



Questions?

Email: Craig.Schumacher@itd.idaho.gov

NIST: <http://www.nist.gov/cyberframework/>