Using Metrics to Gain Management Support for Cyber Security Initiatives

Craig Schumacher

Chief Information Security Officer

Idaho Transportation Dept.

January 2016

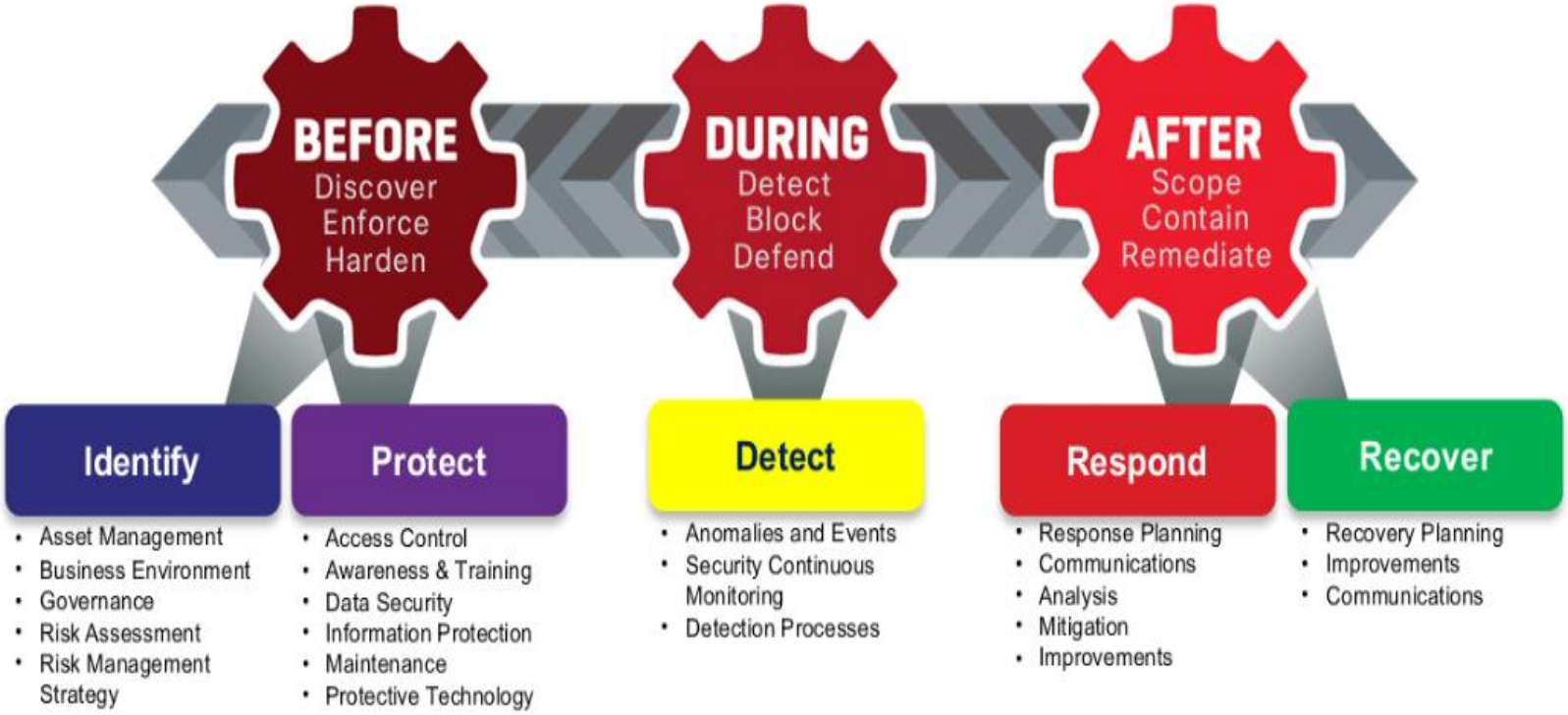
Why Metrics Based on NIST Framework?

- Help us better understand, manage, and reduce cyber security 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 an objective quantitative manner the status of the program and where improvements are needed.

The Strategic Perspective of the Functions

The Threat-Centric Security Model

Aligning with the Cybersecurity Framework Core



NIST Framework Details

The Framework Core defines Function, Category, Subcategory and Reference Documents.

Category	Subcategory	Informative References
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	· **CCS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
	ID.AM-2: Software platforms and applications within the organization are inventoried	· **CCS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
	ID.AM-3: Organizational communication and data flows are mapped	· **CCS CSC** 1 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
	ID.AM-4: External information systems are catalogued	· **COBIT 5** APO02.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	· **COBIT 5** APO03.03, APO03.04, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **COBIT 5** APO01.02, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

NIST Tiers

- Rated by Tiers

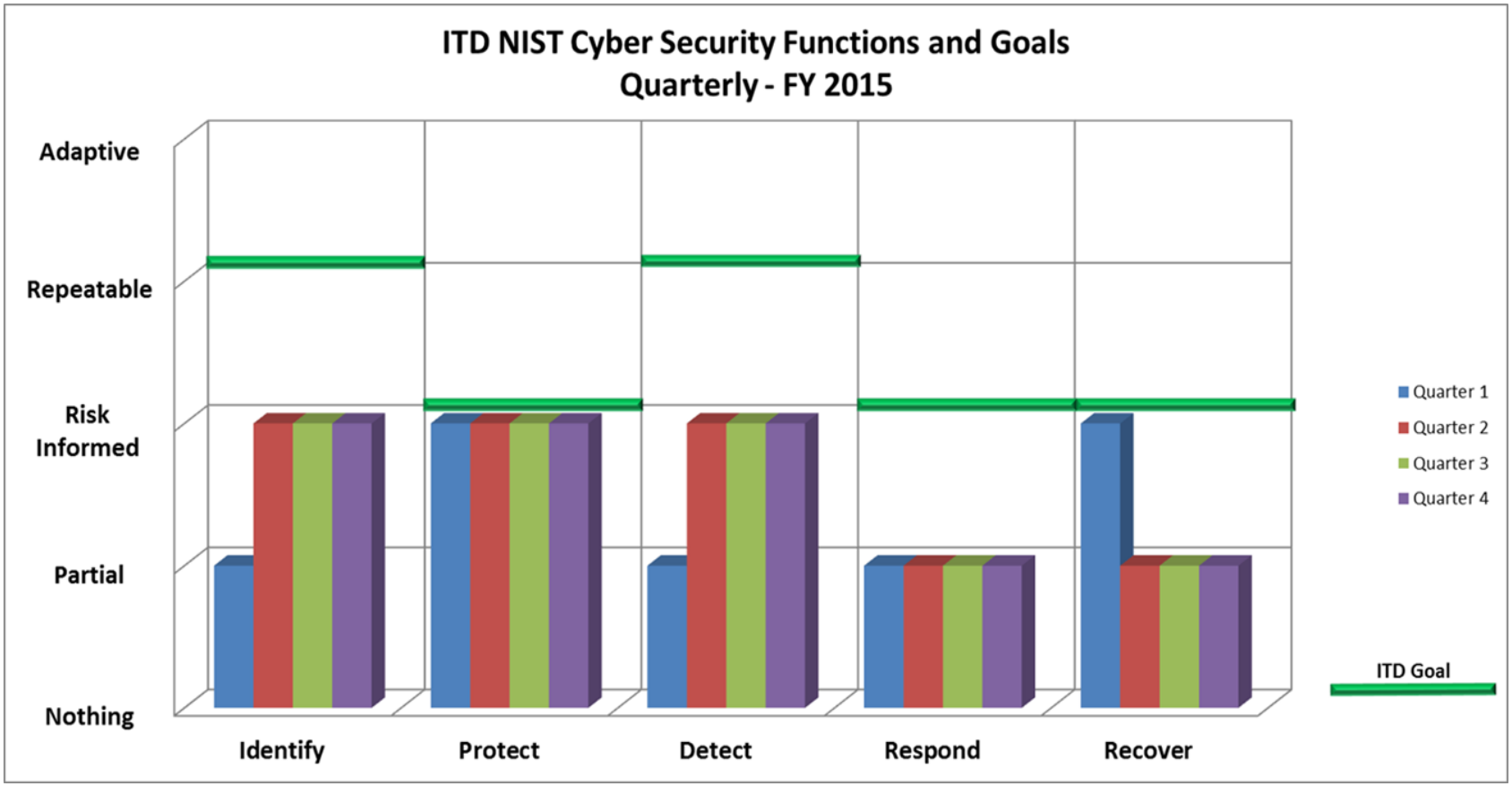
Tier Score	Tier
0	Nothing
1	Partial
2	Risk Informed (Communicated)
3	Repeatable
4	Adaptive

How did we measure our progress

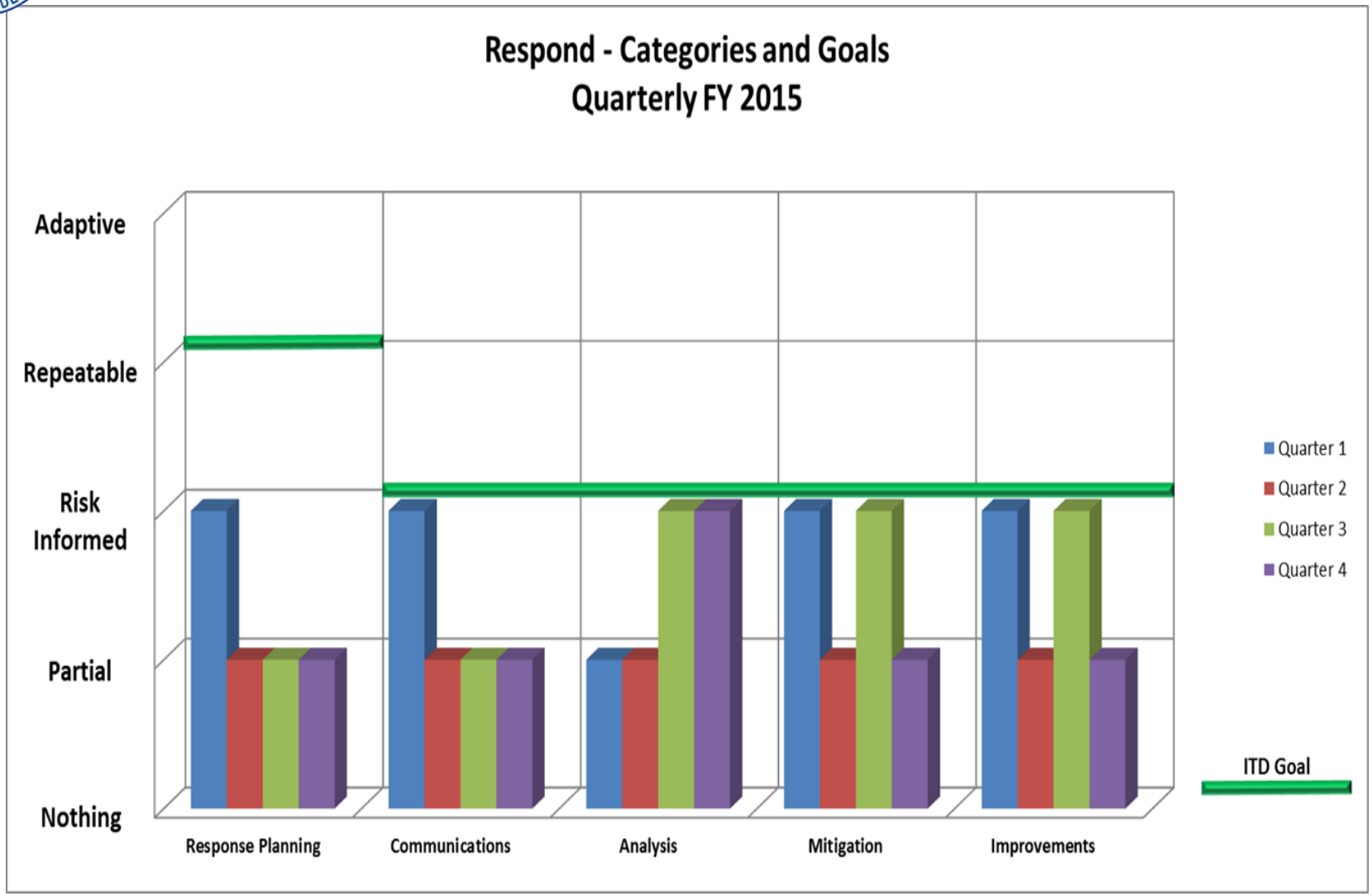
- Established a method of scoring by using the numeric value of the Tier (0 through 4) of Sub Category and Control Documents.
- Developed a matrix (Excel spreadsheet) to capture the score.
- Created the Baseline and Target Profile based on the framework.
- Developed a graphic representation of the scores assessed quarterly.

Visual Management – Key to Success

Establish a Baseline Profile, set Target Profile, evaluate progress and communicate progress and risks



Interpreting the Metrics



Respond

Categories and Subcategories

- **Response Planning RS.RP:**
  - RS.RP-1: Response plan is executed during or after an event CP-2, CP-10, IR-4, IR-8
- **Communications RS.CO:**
  - RS.CO-1: Personnel know their roles and order of operations when a response is needed CP-2, CP-3, IR-3, IR-8
  - RS.CO-2: Events are reported consistent with established criteria AU-6, IR-6, IR-8
  - RS.CO-3: Information is shared consistent with established criteria CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
  - RS.Co-4: Coordination with Stakeholders occurs consistent with response plans CP-2, IR-4, IR-8

The Reference Documents

NIST Special Publication 800-53

"Security and Privacy Controls"

Reference	Potential	Name
IR-4	38	Incident Handling
IR-8	26	Incident Response Plan
CP-2	19	Contingency Plan
SI-4	16	Information System Monitoring
AU-6	12	Audit Review, Analysis, Report
RA-5	10	Vulnerability Scanning
CA-7	9	Continuous Monitoring

Conclusions

- ITD budget cycle runs 2 years in advance and using this method can justify the budget increase requests.
- Long range planning is affected by current events but still can be done effectively.
- Priorities are identified by gaps of 1 or more tiers.
- Leveraging the Potential of control documents assures that the metrics will show the results of the planning.
- By using this method I can predict which categories will show a tier increase because of the investment.

Lessons Learned

- Team was improving categories we were already strong on, not on the categories we were weakest on.
- Our baseline was too optimistic.
- Sometimes scores drop because we are improving the process and sometimes because of the ever changing world of cyber security.
- We need to plan long term for the budget, but be flexible in responding to present needs.

Questions?

Email: Craig.Schumacher@itd.idaho.gov

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