The Relationship Between Regulators and Power Utilities:

Michael Colao, CIPP/US

Evaluating the Prudency of Cybersecurity Investments

APS – Background Information

-Arizona Public Service

- Founded in 1885 as the Phoenix Light and Fuel Company
- Service territory of 11 counties within Arizona from metropolitan Phoenix to the Grand Canyon
- 4,000 MW of generating capacity
- Operators of America's largest nuclear generating station, Palo Verde
- Generate electricity for nearly 3 million Arizona customers and businesses
- 6,300 employees and 2,000 temporary contractors

Who Are APS' Regulators?

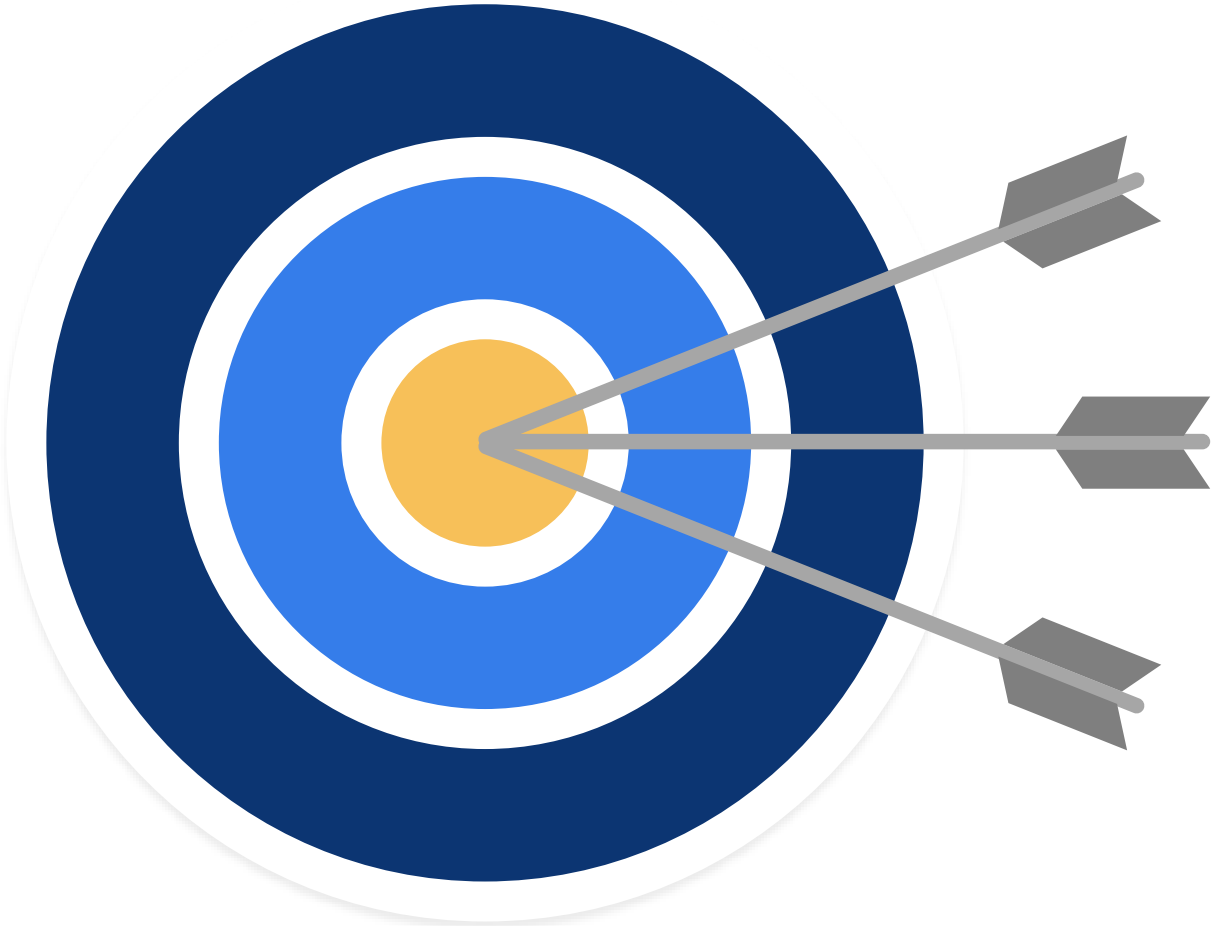
State

Arizona Corporation Commission (ACC)

Federal

1. Federal Energy Regulatory Commission (FERC)
2. Western Electricity Coordinating Council (WECC)

Who Are APS' Regulators (continued)?



ACC – State enforcement; safety and security thru dockets

FERC - seeks comprehensive solutions to potential threats to infrastructure from cyber and physical attacks; delegates authority to WECC

WECC – Enforces framework requirements (CIP) thru civil penalties

Interaction Between Regulators and What to Expect……

Keep line of communication open; approach regulators often

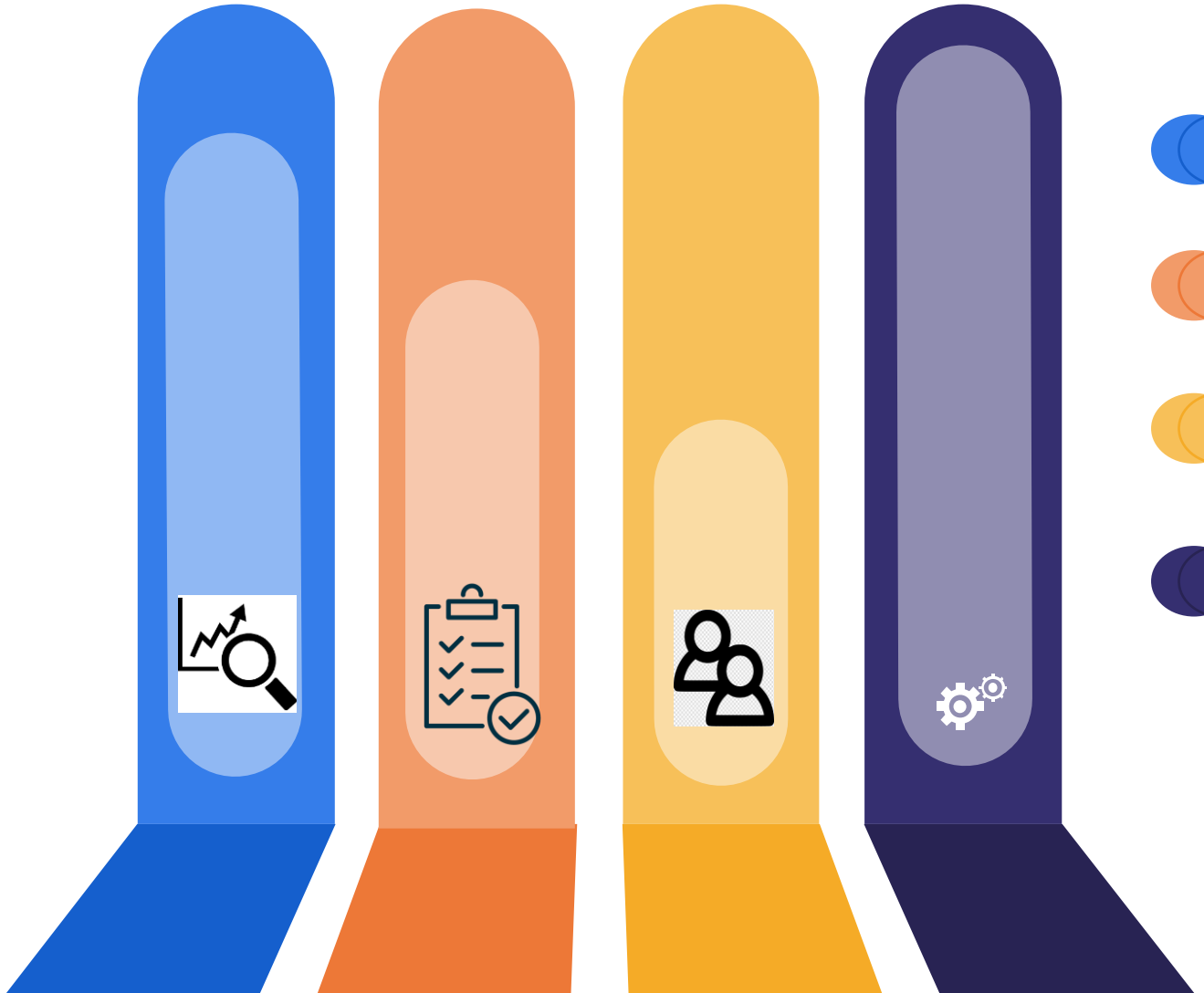
3-year cycle of audits

Regulators will set the tone; generally friendly but distant

Your internal Regulatory Department is the Bridge

Frameworks provide guidance; consultations are your friend

Utility Perspective – Managing Benchmarks and Effectiveness of Cyber Security Program



Set Metrics & Measure (recurring)

Assessments (C2M2)

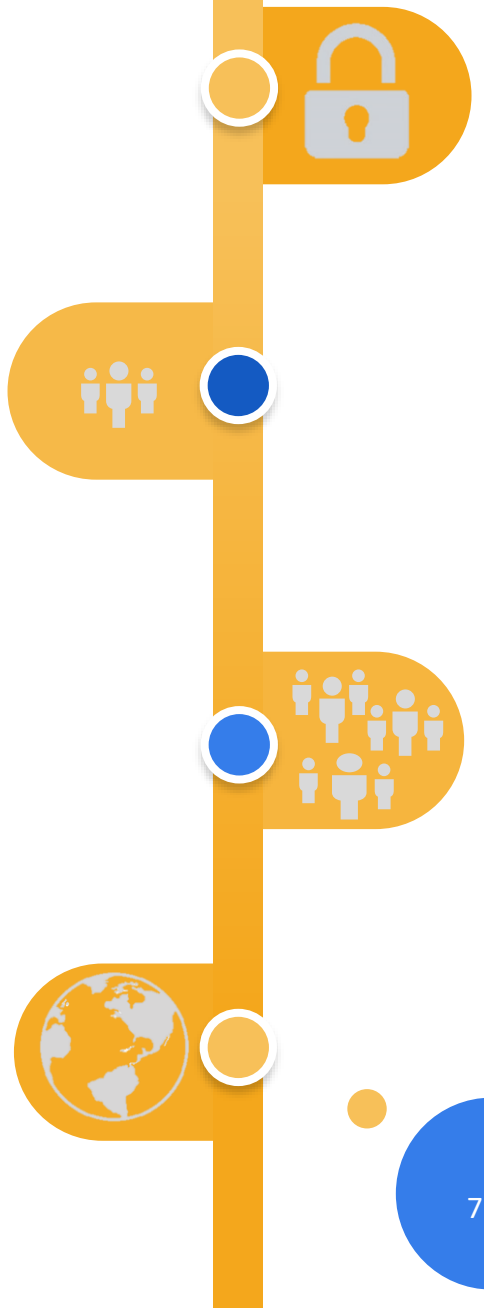
Peer Groups (UNITE)

Frameworks

- NIST 800-53
- NIST Privacy Controls
- SOX (GITC controls)

Is it Possible to Evaluate Your Cybersecurity Investment?

Risk Register	Peer Groups	Regulatory Fines	Reputational Harm
-Identity processes, programs or technology putting your data at risk	-Either formal or ad hoc discussions with colleagues inside the utility industry to benchmark your program	-Fines arise from audit findings or self-reports between audit cycles	-A cyber event, even minor, will lead to reputational damage; a robust program will mitigate this harm



Risk Ranking Criteria - APS

Risk - Cybersecurity Risk Ranking Criteria

Authored by RESSA, ALEX/Z11102 • 7mo ago • 6 Views •

Cybersecurity uses the following formula and criteria for calculating a risk score. The criteria is provided by the APS Enterprise Risk Committee.

Formula:

√ **[(Likelihood x Highest Impact) / 2]**

This results in a score between 1 – 5.

Example:

Likelihood: 3
Financial Impact: 6
Operational Impact: 8
Reputational Impact: 4

Score Calculation: √ **[(3 x 8) / 2]** → √ **[24 / 2]** → √**12** → **3.5**

Explanation - The Likelihood was a 3 and the highest impact listed was Operational at 8.

Criteria:

Likelihood

1	Requires specialized attack and knowledge by skilled adversary.
2	Requires specialized attack OR detailed knowledge of APS/PNW by a skilled adversary.
3	Requires a moderately skilled attacker OR can be realized through inadvertent acts (e.g., social engineering) without compensating controls.
4	Requires relatively low attacker skill (e.g., modify attack code available from the Internet) OR can be realized through simple misconfiguration without compensating controls.
5	Attack is trivial to execute or condition is currently pervasive across the company.

Financial Impact

2	Very Limited (< $2M)
4	Limited ($2 - $5M)
6	Moderate ($5 - $15M)
8	Significant ($15M - $25M)
10	Major (>$25M)

Operational Impact

2	Very Limited, No or local outages of a very small duration
4	Limited, Local outages caused by pole collapse, pole fires and transformer problems usually impacting a smaller geographical area or an event which has a reasonable probability of limited negative impact to the Company's operational objective.
6	Moderate, Outage arising from a major line or circuit outage impacting greater than 50,000 customers or an event which has a reasonable probability of moderately negatively impacting the Company's operational objective.
8	Significant, Potential for rolling blackouts at times when the demand exceeds supply (large geographical area affected) or an event which has a reasonable probability of significantly negatively impacting the Company's operational objective.
10	Major, Potential for grid instability leading to large scale blackouts due to generation or transmission related voltage and frequency instabilities.

THANK YOU

Questions??

Michael Colao, CIPP/US

michael.colao@aps.com