OEB Cyber Security Framework Elements

MEARIE 2017 Risk Management Conference

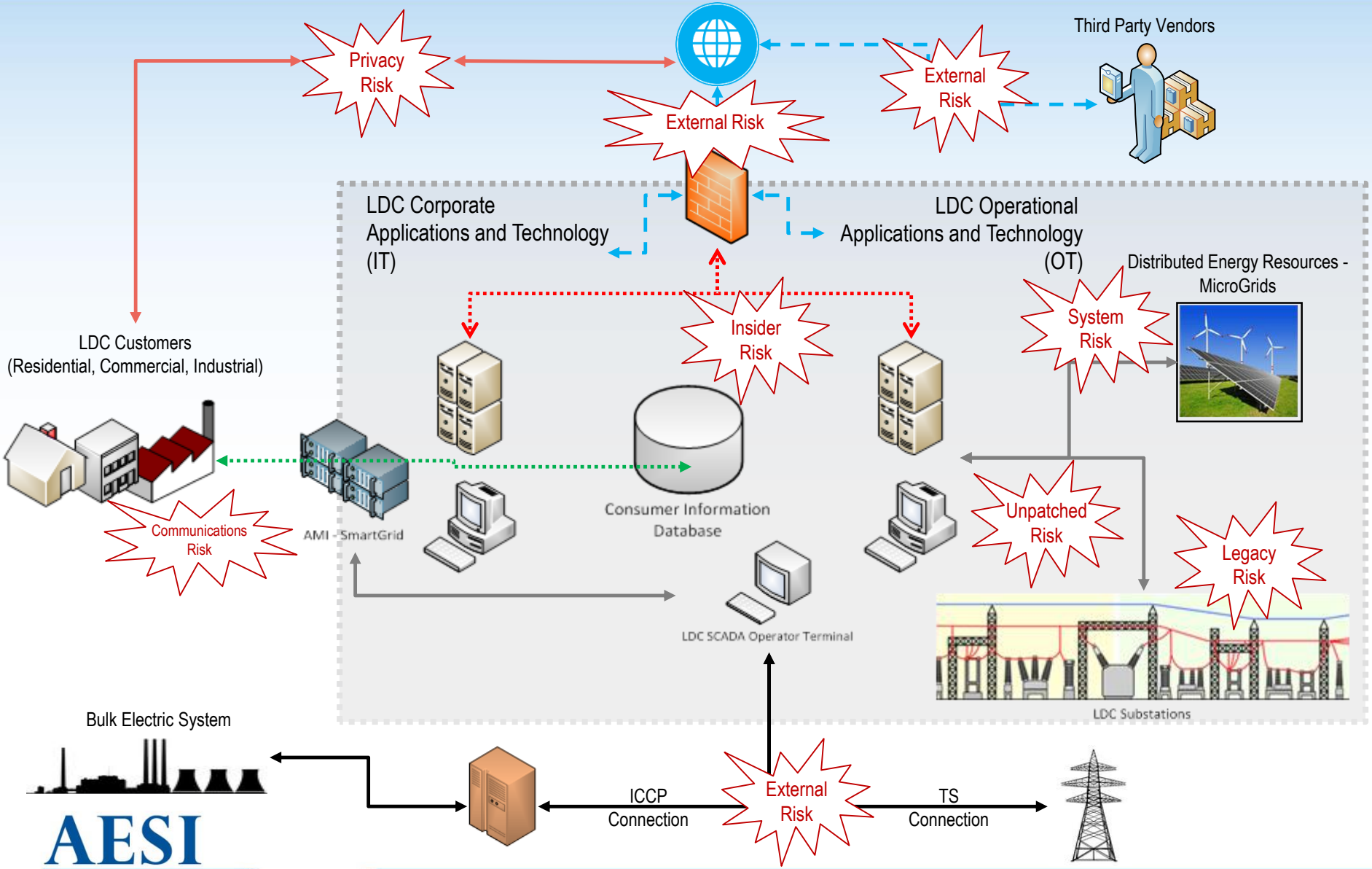
Doug Westlund

Senior VP, AESI

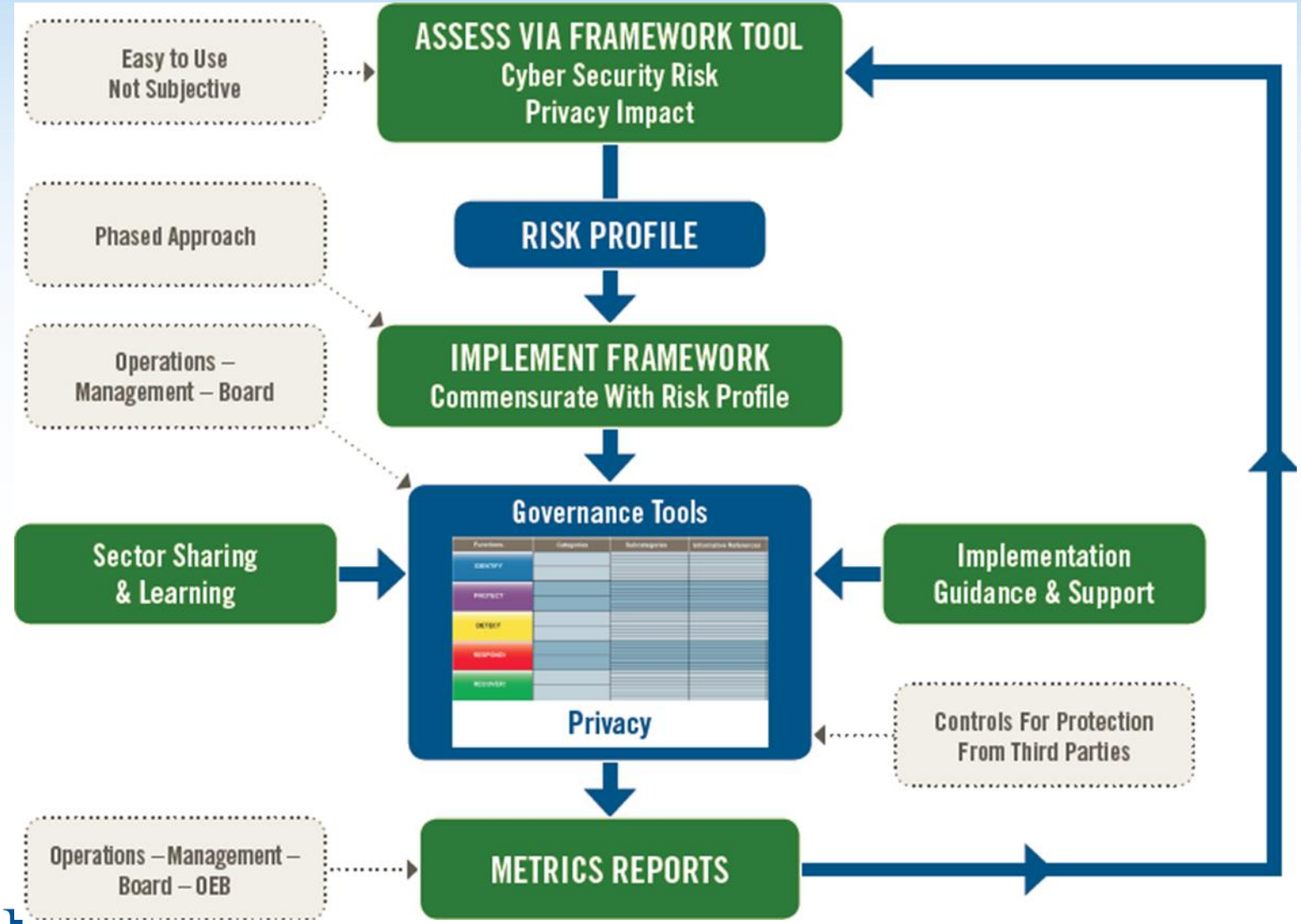
Discussion Topics

- The Framework
- Risk Profiling
- Application of Security Controls
- Sector Sharing & Learning
- Q & A

The LDC Attack Surface



The Framework



Foundation: NIST Cybersecurity Framework

Functions	Categories	Subcategories
IDENTIFY		
PROTECT		
DETECT		
RESPOND		
RECOVER		

Privacy Integrated Into Framework

Fair Information Principles (FIPs) / PIPEDA are compatible with NIST

- [Accountability, Consent, Limiting Collection…]

NIST Framework does not deal with Privacy in any detail; however, were incorporated because LDCs should already doing this.

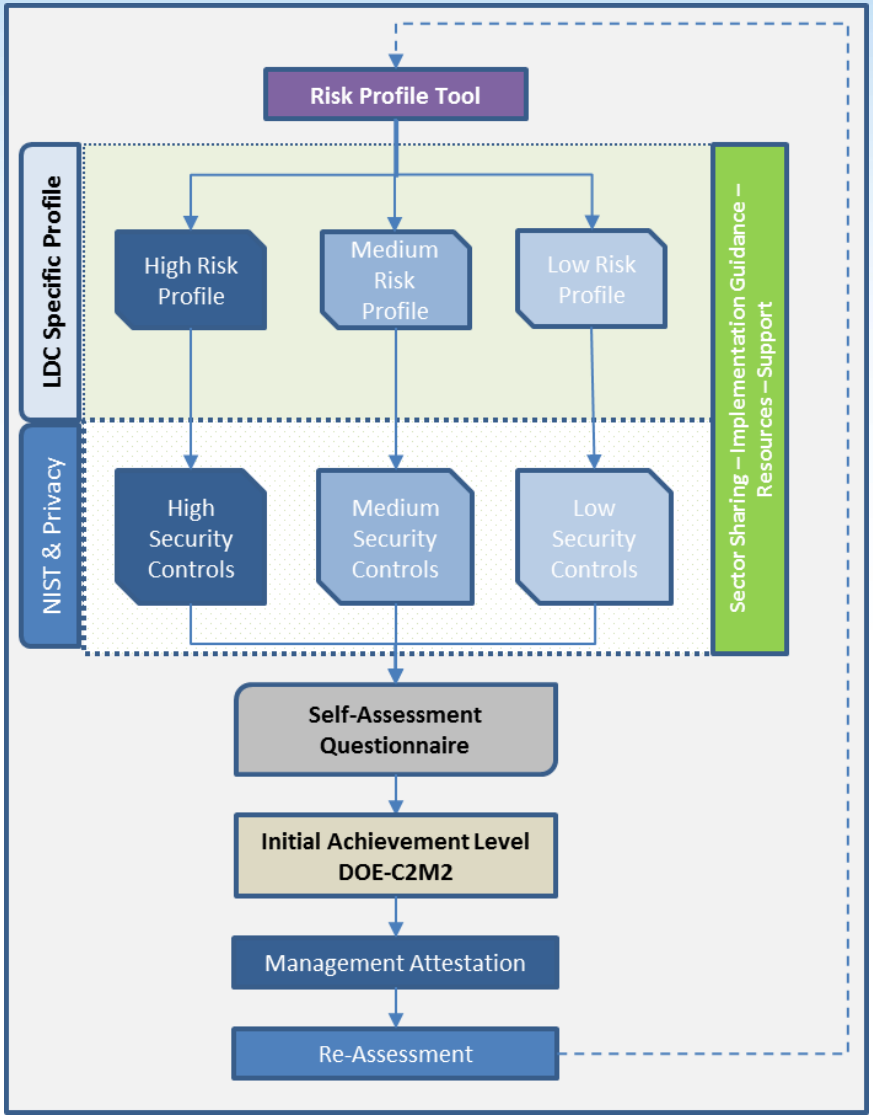
- [ID.GV-3: “Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations are understood and managed”]

FIPs have been embedded into the Framework by:

- Building privacy questions into the Risk Profile Tool
- Layering privacy controls onto the NIST controls

The Risk Profile Tool

- Risk Profile tool creates an LDC Specific Profile
- Each Profile aligns with specific security controls
- Each LDC self-assesses compliance with the security controls in Stage 1
- Initial achievement level is defined using DOE-C2M2 Implementation levels
- LDC CEO provides attestation



Risk Profile Tool

Question	Response	Risk Factor
Q1. Do you have a SCADA System ?	Response	RF1
Q2. How many customers do you serve ?	Response	RF2
Q3. Do you process credit card transactions or pre-authorized bank payments ?	Response	RF3
. . .		
Qn.	Response	RFn
		Total Risk Factor

Specifies

High Risk Profile

Medium Risk Profile

Low Risk Profile

Risk Profiles

Low Risk: Baseline for all

- Controls will not require major investments in technology or specialized resources to implement

Medium Risk: Adds to Baseline

- Additional controls to address level of risk
- Requires some investments (technology & resources) to implement

High Risk: Builds on Baseline

- Increased number of controls to address high-risk
- Requires investments (technology & resources) to implement

Application of the Security Controls

Function	Category	Subcategory	High	Med	Low
IDENTIFY (ID)	**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	✓	✓	✓

Function	Category	Subcategory	High	Med	Low
DETECT (DE)	**Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.**	**DE.CM-4: Malicious code is detected**	✓	✓	

Function	Category	Subcategory	High	Med	Low
RESPOND (RS)	**Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.**	**RS.AN-3: Forensics are performed**	✓		

Role of the LDC Board and Executive Team

Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established
	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
	ID.GV-P1: A policy is established for collection, use and disclosure of customer personal and proprietary information, including requirements for consent and notification
	ID.GV-P2: A policy is established for retention and disposal of customer personal or proprietary information
	ID.GV-P3: Governance and risk management processes address privacy risks
	ID.GV-4: Governance and risk management processes address cybersecurity risks. The Executive Team and Board are actively involved and supportive of the Cyber Security Program.

Self Attestation by the LDC CEO

☐	**Compliant:**	All sections of the NIST subcategory SAQ are complete. All questions were answered affirmatively, resulting in an overall **COMPLIANT** rating; illustrating overall compliance
☐	**Non-Compliant:**	Not all sections of the NIST subcategory SAQ are complete, or not all questions are answered with positive affirmation, resulting in an overall **NON-COMPLIANT** rating **Target Date** for Compliance will be set and remediation activities outlined

Completing the Self-Assessment Questionnaire

For each question, there is a choice of responses to indicate your LDC's status regarding that requirement. A description of the meaning for each response is provided in the table below.

Yes	The expected testing has been performed, and all elements of the requirement have been met
Yes with CCW	The expected testing has been performed, and the requirement has been met with the assistance of a compensating control.
No	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.
N/A	The requirement does not apply to the organization's environment.
Not Tested	The requirement was not included for consideration in the assessment, and was not tested in any way

Sector Sharing and Learning

- **Cyber Security Information Sharing Forum (CSIF) Concept**
- **LDC Collaboration Forums**
  - Existing e.g. USF, CHEC, GridSmartCity, EDA Districts
  - New within the CSIF
- **Framework implementation guidance**
- **Potential cross-border sharing**

Doug Westlund

dougw@aesi-inc.com 905-875-2075 ext 278