Using the NIST Cybersecurity Framework to Guide your Security Program

August 31, 2017

Presenters:

Allie Russell, Conexxus

Kara Gunderson, DSSC Chair, CITGO Petroleum

Chris Lietz & Bob Post, Coalfire

CONEXXUS
solve forward

Agenda

- Housekeeping
- Presenters
- About Conexxus
- Presentation
- Q & A

Housekeeping

This webinar is being recorded and will be made available in approximately 30 days.

- YouTube (youtube.com/conexxusonline)
- Website Link (conexxus.org)

Slide Deck

- Survey Link – Presentation provided at end

Participants

- Ask questions via webinar interface
- Please, no vendor specific questions

Email: **info@conexxus.org**

Presenters

Conexxus Host

Allie Russell

Conexxus

arussell@conexxus.org

Moderator

Kara Gunderson

Chair, Data Security Committee

POS Manager, CITGO Petroleum

kgunder@citgo.com

Speakers

Chris Lietz

Principal, Coalfire

Chris.Lietz@coalfire.com

Bob Post

Sr. Director, Coalfire

Bob.Post@coalfire.com

Speakers

Chris Lietz MBA, CISSP, CISA, CISM, CRISC, CGEIT, CTPRP

Principal, Cyber Risk Advisory

Coalfire

- 30+ years experience in cybersecurity, predictive analytics, and technology; 8 years with Coalfire
- Long-time participant in Conexxus Data Security Committee activities
- Advisor to clients in retail, insurance, banking and technology

Speakers

Bob Post, CISSP

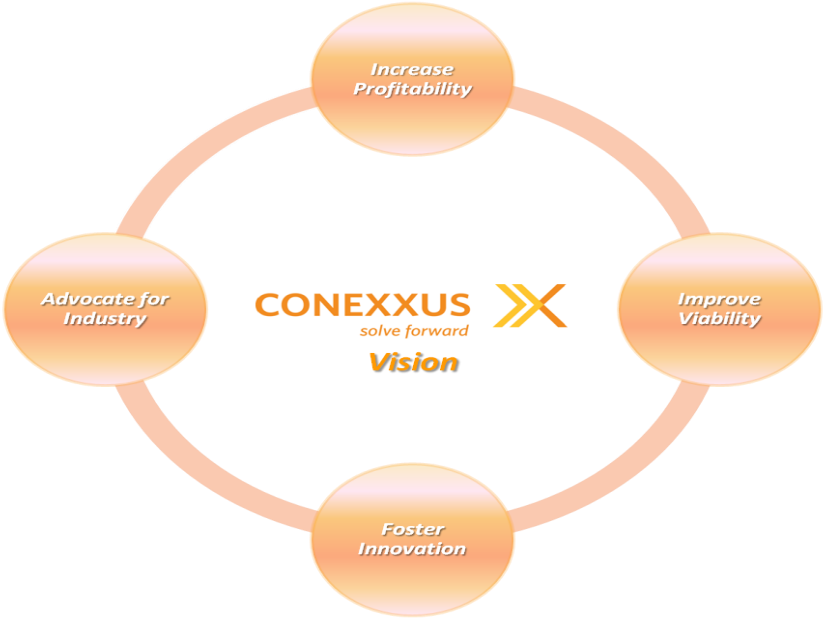
Senior Practice Director, Cyber Risk Advisory

Coalfire

- 30 years experience in cybersecurity, critical infrastructure protection, emergency preparedness, and operations security.
- Works with senior leaders on cybersecurity strategy, governance, risk management and compliance issues. Bob's client set includes biotechnology firms, internet media companies, investment firms, and government contractors.
- Former CEO and Founder of Crossroads Cyber Solutions, Inc.; Former Senior Vice President, Booz Allen Hamilton, Inc.

About Conexxus

- We are an independent, non-profit, member driven technology organization
- We set standards…
  - Data exchange
  - Security
  - Mobile commerce
- We provide vision
  - Identify emerging tech/trends
- We advocate for our industry
  - Technology is policy



2017 Conexxus Webinar Schedule*

Month/Date	Webinar Title	Speaker	Company
July 27, 2017	Third Party Risk Management: How to Identify and Manage Data Security Risks from your Vendors	Sam Pfanstiel	Coalfire
August 31, 2017	Using the NIST Cybersecurity Framework to Guide your Security Program	Chris Lietz, Bob Post	Coalfire
September 28, 2017	Things & Impact of Bring Your Own Device to the Workplace	Bradford Loewy Jeff Gibson	Dover Fueling ControlScan
November, 2017	New Technologies for Addressing Payment Risk: A Survey of Payments Security Landscape	TBD	Coalfire (other DSSC member(s) TBD)
December 2017	Conexxus: EB2B White Paper Presentation	TBD	EB2B WG

2018 Conexxus Webinar Schedule*

Month/Date	Webinar Title	Speaker	Company
January 2018	Securing and Penn Testing your Mobile Payment App	Denis Sheridan	Citigal
February 2018	Unified threat management: What is it and why is it important?	Thomas Duncan	Omega
March 2018	Penetration Testing: How to Test What Matters Most	Sam Pfanstiel & Coalfire Lab Personnel	Coalfire
May 2018	QIR Program Update	Chris Bucolo	ControlScan

At the NACS Show
October 17-20, 2017
Chicago, IL
Booth 4384

Agenda

- NIST CSF Overview (Chris)
- Implementing the CSF (Bob)
- Resources & Recommended Actions
- Q&A

NIST CSF OVERVIEW (CHRIS)

Going-in Assumptions

1. Every enterprise is increasingly aware of cyber risk, and is seeking to ‘manage it’ through:
   - Policies, procedures and other administrative controls
   - Technology-based controls
   - Insurance (aka, ‘risk transfer’)
   - Risk acceptance

2. Cyber is an enterprise-wide risk management issue
   - It is much broader than the PCI DSS
   - It is a business issue, not only a technology issue
   - Legislators and regulators may take action

3. Listeners may be looking for a:
   - A place to start their cybersecurity programs, or
   - A way to communicate with stakeholders and set priorities & budgets
   - A way to measure progress
   - A way to get risk under (sufficient) control

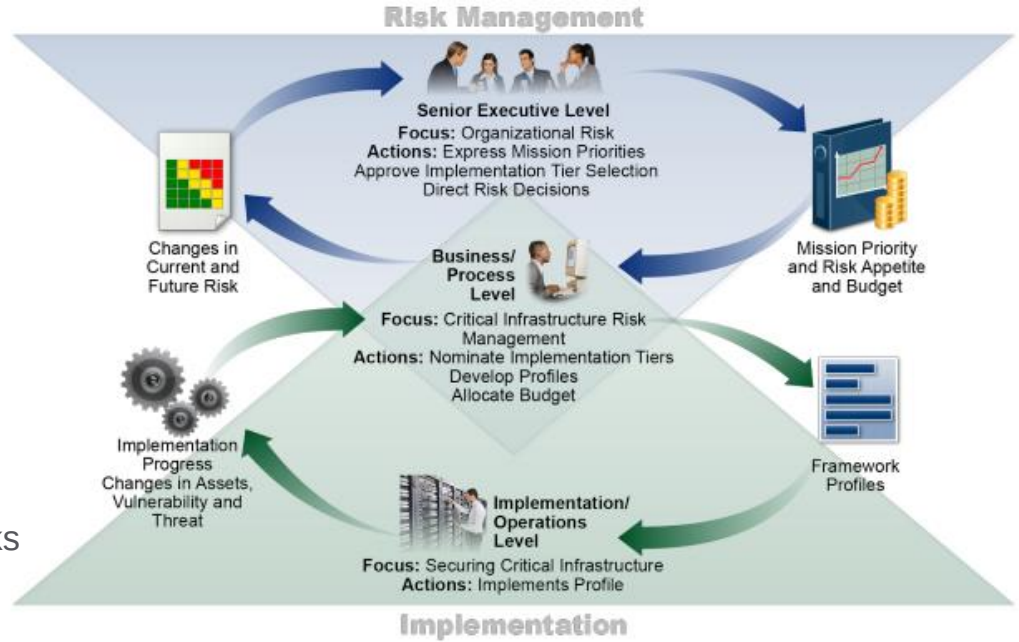
Executive Order (EO) 13636

- Repeated cyber intrusions demonstrated the need for improved cybersecurity
- February 12, 2013: President Obama issued Executive Order (EO) 13636 - Improving Critical Infrastructure Cybersecurity
- National Institute of Standards and Technology (NIST) developed the “Framework for Improving Critical Infrastructure Cybersecurity” (aka, the “CSF”)
  - Version 1.0 released in February 2014
  - Draft Version 1.1 released in January 2017

SOURCE: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Framework Overview

- Intent
  - Voluntary
  - Adaptable and flexible
- Leverages standards, methodologies, and processes
  - Not a compliance checklist or control framework
  - Not a law or regulatory mandate
- Risk-based approach
  - Focused on top-down high impact risks
  - Connects executive, business, and security operations



SOURCE: https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf

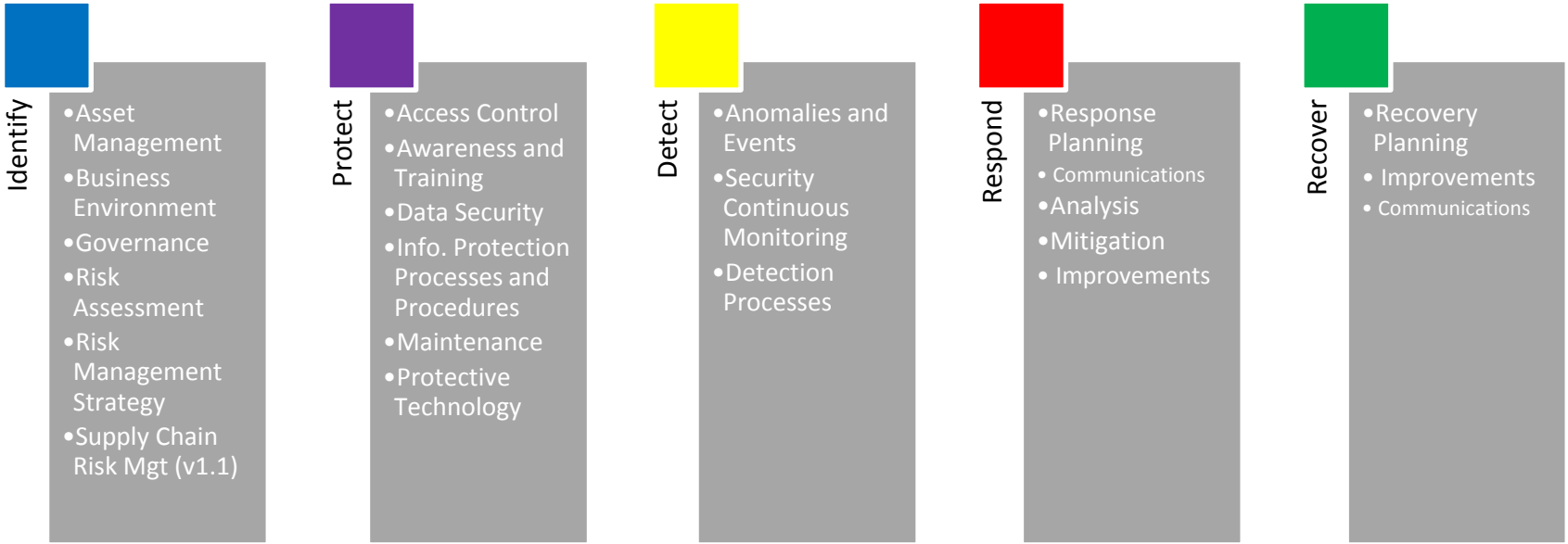
Components and Usage

Component	Description
Framework Core	Consists of five (5) functions (Identify, Protect, Detect, Respond and Recover) and includes activities, desired outcomes and applicable references.
Implementation Tiers	Provides context and identifies the degree in which practices exhibit the characteristics defined in the framework. Tiers range, from Tier 1 Partial to Tier 4 Adaptive.
Profiles	Outcomes based on business needs. This is the analysis of current and target profiles that help determine the prioritization of efforts based on risk.
Implementation Guidance	Uses a seven-step process that is iterative and flexible.

Framework Core (Illustration)

SOURCE: Todd Marcinik, 2017 GRC Conference

Framework Core



SOURCE: Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, NIST . January 2017

Framework Core (cont.)

Function	Category	Subcategory	Industry Standards and Alignment
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	· **CCS CSC** 16 · **COBIT 5** DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.5.1 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 · **NIST SP 800-53 Rev. 4** AC-2, IA Family
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	· **CCS CSC** 12, 15 · **ISA 62443-2-1:2009** 4.3.3.7.3 · **ISA 62443-3-3:2013** SR 2.1 · **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 · **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16

SOURCE: Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, Feb 2014

Implementation Tiers

Tier	Description
Tier 1: Partial	• Risk Management Process – Informed risk practices. Reactive, ad-hoc risk approach. • Integrated Risk Management Program – Limited institutional awareness. Risk management in place but irregular. • External Participation – Lacks process to coordinate and collaborate.
Tier 2: Risk Informed	• Risk Management Process – Approved risk management practices but not organization-wide. Priorities informed by stakeholder goals and corporate risk decisions. • Integrated Risk Management Program – Organization has cyber security risk awareness but not an institutionalized approach. • External Participation – Organization has not formalized capabilities to interact and share information.
Tier 3: Repeatable	• Risk Management Process – Risk management practices formally approved, expressed as policy, regularly updated. • Integrated Risk Management Program – Organization-wide approach to managing cyber security risk. Risk-informed policies, processes and procedures are defined and reviewed. • External Participation – Organized understands dependencies and partners. Receives information that enables collaboration and risk-based response decisions.
Tier 4: Adaptive	• Risk Management Process – Implementation Guidance uses a seven-step process that is iterative and flexible. • Integrated Risk Management Program – Organization risk approach with situational awareness integrated into culture. • External Participation – Active sharing with partners to proactively learn and benefit the community.

SOURCE: Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 NIST , Feb 2014

IMPLEMENTING THE CSF (BOB)

Implementing the CSF

Step 1 - Prioritize and Scope

- What are you trying to assess?
  - Enterprise
  - Business Unit
  - Business Process
- How does the assessment target align with overall goals and priorities?

Step 2 - Orient

- What are the supporting IT systems and assets
- What are the relevant legal, regulatory, and contractual requirements?
- Has a risk strategy been developed and implemented?

Step 3 – Create a Current Profile

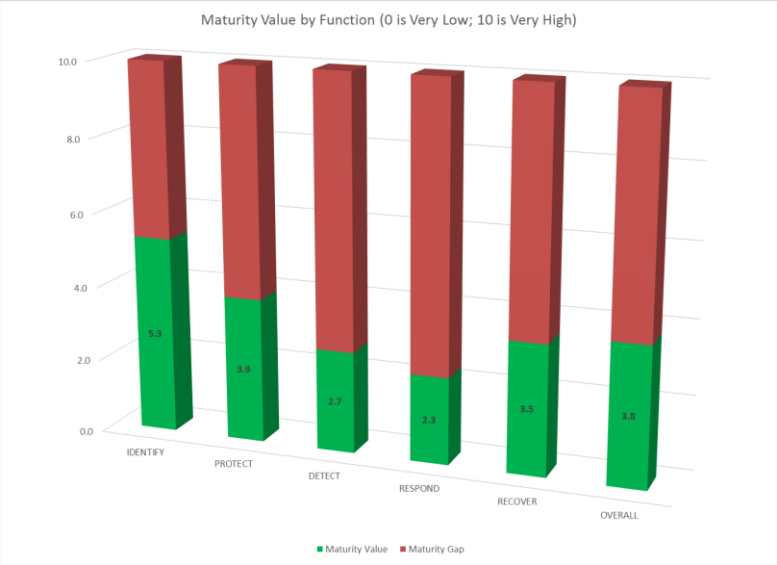
- Functions organize basic cybersecurity activities
- Categories are groups of outcomes (Asset Management)
- Subcategories are specific outcomes of management or technical activities

Step 4 – Assess Risk

Risk Area	High	Medium	Low
Legal & Regulatory	The company handles customer/employee information of a sensitive and personal nature to include PII and PHI as defined by law/regulations where the company conducts operations.	The company handles customer/employee information of a personal but not sensitive nature to as defined by law/regulations where the company conducts operations.	The company does not handle personal data other than those of the people employed by the organization.
Productivity	The company employs more than 100 employees who have a daily need to access business applications and services.	The company employs more than 50 employees who have a daily need to access business applications and services.	The company employs less than 10 employees who have a daily need to access business applications and services.
Financial Stability	Yearly revenues exceed $xxx and/or financial transactions with third parties or customer are taking place as part of the business approval process.	Yearly revenues do not exceed $xxx M.	Yearly revenues do not exceed $xx M.
Reputation/Loss of Customer Confidence	Unavailability or Service Quality directly impacts the business or/and over 70% of the customer base has online access to business products or services.	Unavailability or Service Quality can indirectly have impact on the business or/and less than 5% of the customer base has online access to business products or services.	Unavailability or Service Quality cannot directly or indirectly have impact on the business or result in the loss of revenues.

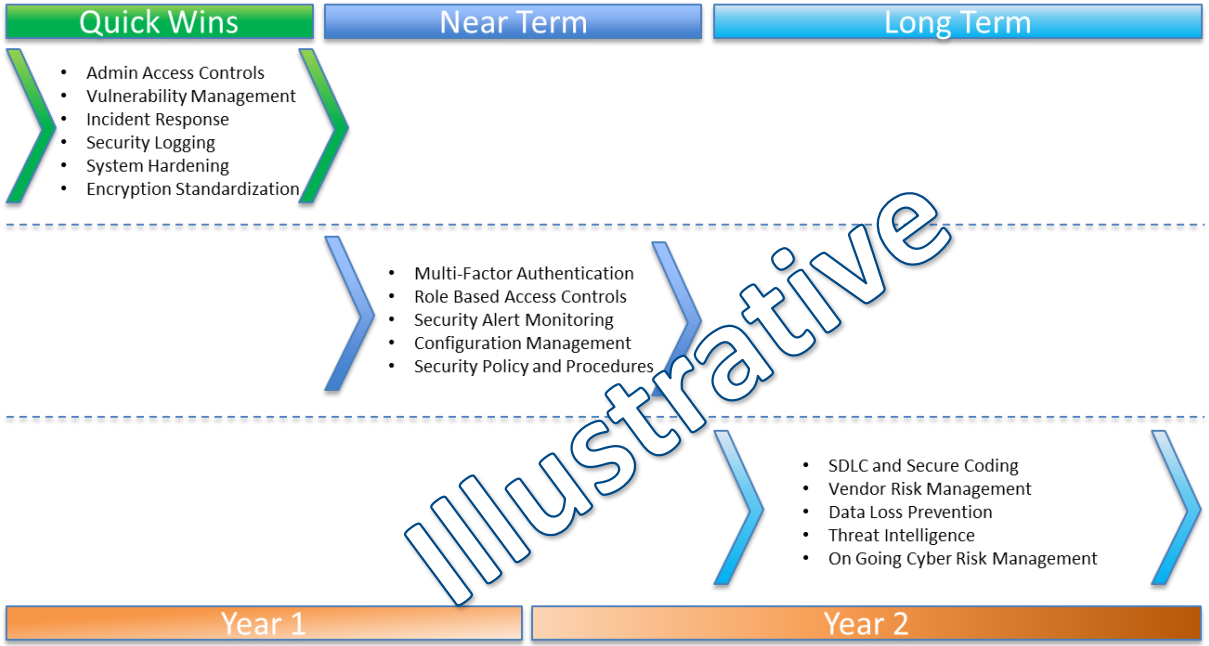
Step 5 – Create Target Profile

Step 6 – Determine, Analyze, and Prioritize Gaps



Summary of Cyber Risk Controls Maturity Level: Low					
Function / Category	# of Category Controls	Control Testing Status			
		Satisfied	Partially Satisfied	Not Satisfied	Incomplete
IDENTIFY	24	5	11	8	0
Asset Management	6	0	5	1	0
Business Environment	5	4	1	0	0
Governance	4	1	3	0	0
Risk Assessment	6	0	2	4	0
Risk Management Strategy	3	0	0	3	0
PROTECT	34	2	16	14	2
Access Control	5	0	5	0	0
Awareness and Training	5	0	2	3	0
Data Security	6	1	1	4	0
Information Protection Processes and Procedures	12	1	6	5	0
Maintenance	2	0	0	0	2
Protective Technology	4	0	2	2	0
DETECT	18	0	7	11	0
Anomalies and Events	5	0	2	3	0
Security Continuous Monitoring	8	0	4	4	0
Detection Processes	5	0	1	4	0

Step 7 – Implement Action Plan



RESOURCES & RECOMMENDED ACTIONS

Resources

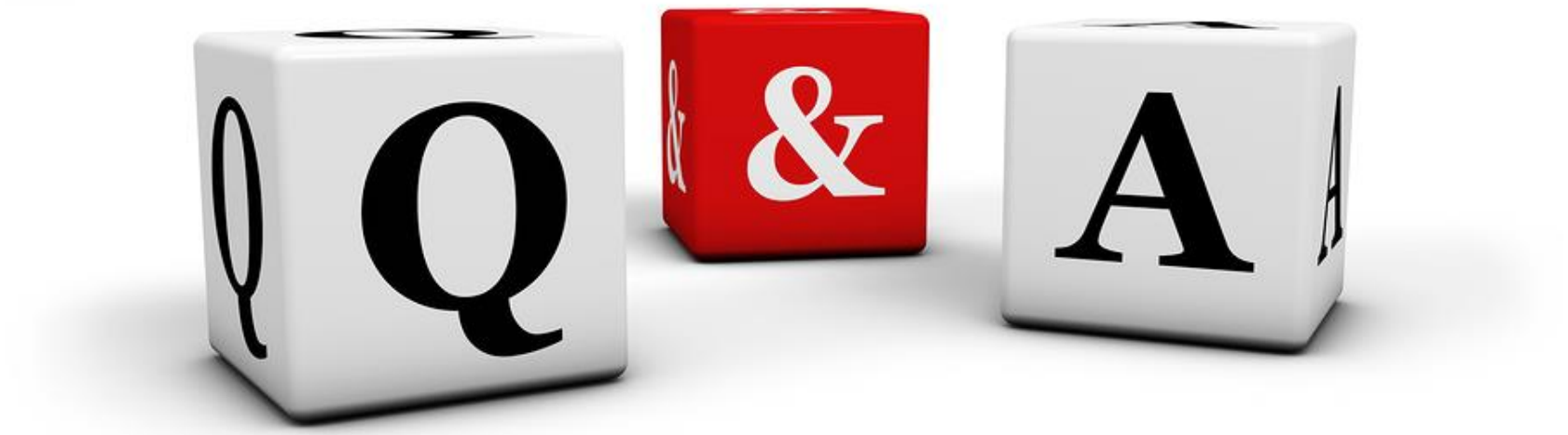
- NIST Cybersecurity Framework
  - http://www.nist.gov/cyberframework/
- ISACA
  - http://www.isaca.org/cyber/
- FFIEC
  - https://www.ffiec.gov/cybersecurity.htm
- Information Security and Risk
  - NIST SP 800-30, 800-39, 800-53
  - COBIT5 for Risk, COBIT 5 for Information Security
  - ISO 27005, ISO 31000
  - https://www.cisecurity.org/critical-controls/
- NACD
  - Director's Handbook on Cyber-Risk Oversight https://www.nacdonline.org/cyber
- Other
  - How to Measure Anything in Cybersecurity Risk http://www.wiley.com/WileyCDA/WileyTitle/productCd-1119085292.html
  - Measuring and Managing Information Risk: A FAIR Approach: http://www.fairinstitute.org/fair-book

Recommended Actions

1. Review/adopt the NIST CSF

2. Form a team (e.g., a security governance process)

3. Start a CSF-based program that includes:
    1. Scope statement (enterprise, location, department, etc.)
    2. “Crown jewels” inventory (systems, suppliers, assets)
    3. Current profile (where you are at it re: controls)
    4. Risk assessment (likelihood/impact of named risks)
    5. Target profile (where you want to be re: controls)
    6. Prioritize & act (investments, projects, tests)
    7. Implement



CONEXXUS
solve forward

- Website: www.conexxus.org
- Email: info@conexxus.org
- LinkedIn Group: Conexxus Online
- Follow us on Twitter: @Conexxusonline