


# **Acing a Cyber-Security Assessment**

2014 WBA Technology Conference



Ken M. Shaurette  
CISSP, CISA, CISM, CRISC, IAM  
Director IT Services

COMPLIANT. CONSISTENT. CONFIDENT.

## Disclaimer



The views set forth are those of this presenter and do not necessarily reflect the views of the Federal Financial Institutions Examination Council, or those of the Federal Deposit Insurance Corporation.

The presenter is not an examiner nor has he ever been and does NOT have plans to become one anytime soon. He does provide almost 30 years experience from listening to people complain about various regulations.

» "Ken M. Shaurette"

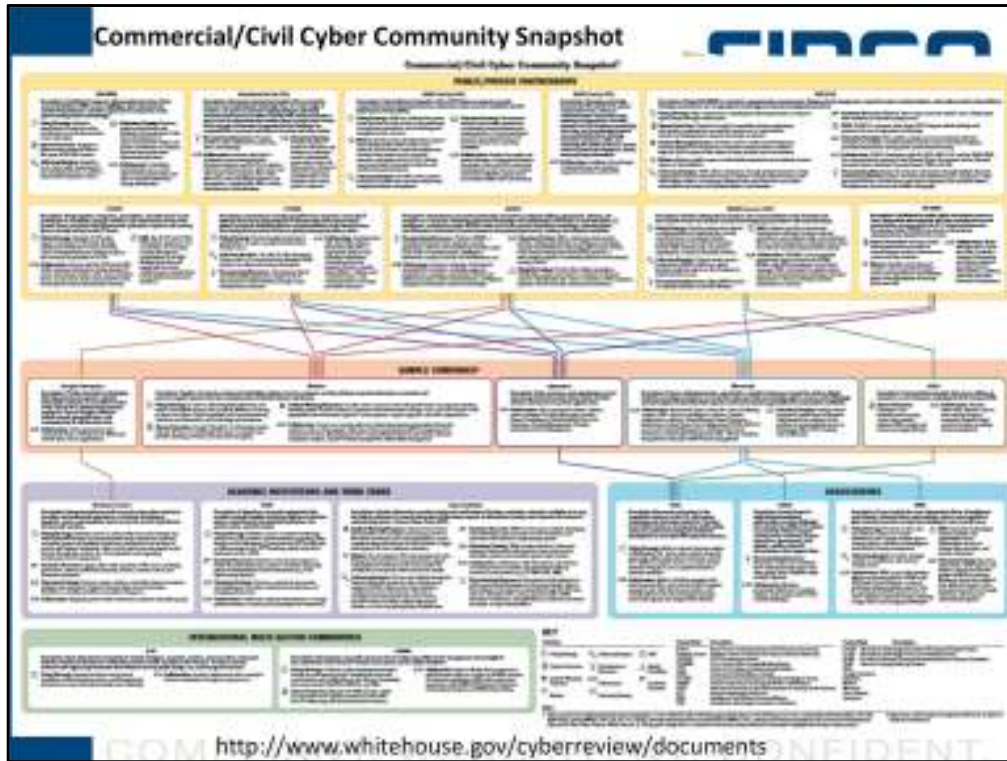
COMPLIANT. CONSISTENT. CONFIDENT.

## Key Barriers to CyberSecurity

- CyberSecurity is still considered just an IT Issue!!!!
- Raising your game faster than the attackers.... Say What?

This creates a communications gap between management in the business and the security teams. Board members and cybersecurity professionals don't necessarily speak the same language in regards to IT security. "Most business leaders do not spend a lot of time talking about ISO standards and NIST framework





[http://www.whitehouse.gov/files/documents/cyber/Comm-Civil\\_CyberSnapshotPoster.pdf#page=1&zoom=auto,-29,1080](http://www.whitehouse.gov/files/documents/cyber/Comm-Civil_CyberSnapshotPoster.pdf#page=1&zoom=auto,-29,1080)



## CyberSecurity Assessment – Background & Timeline


June 2013, FFIEC established - CyberSecurity and Critical Infrastructure Working Group (CCWIG) - Collaborating with .....

May 7, 2014, FFIEC/FS-ISAC Announces pilot program for CyberSecurity Assessments combined with IT Exams and Presents - What Today's CEO Needs To Know About the Threats They Don't See



COMPLIANT. CONSISTENT. CONFIDENT.


to collaborate on this important issue. This group has been coordinating with intelligence, law enforcement, Homeland Security, and industry officials to make sure the member agencies have accurate and timely threat information to assist institutions in protecting themselves and their customers from the growing risk posed by cyber-attacks.



## CyberSecurity Assessments ?


The CyberSecurity Assessment builds upon key aspects of existing supervisory expectations addressed in the *FFIEC IT Handbook* (<http://ithandbook.ffiec.gov/it-booklets.aspx>) and other regulatory guidance:

1. Assesses the **complexity** of an institution's operating environment, including the types of communication connections and payments initiated, as well as how the institution manages its information technology products and services.



COMPLIANT. CONSISTENT. CONFIDENT.

What now, aren't exams enough, why a new assessment of security, what bunch of new regulations will I need to meet now?



## CyberSecurity Assessments ?

The CyberSecurity Assessment .....  
(Key Areas for Preparedness)

2. Assesses an institution's current practices and overall CyberSecurity preparedness, with a focus on the following key areas:
  - Risk Management and **Oversight**
  - **Threat Intelligence** and Collaboration
  - CyberSecurity Controls
  - External Dependency Management (hear **Vendor**)
  - Cyber Incident Management and **Resilience**

COMPLIANT. CONSISTENT. CONFIDENT.

- Ensure your top-level executives are up to speed on emerging threats.
- Be well-versed in existing cybersecurity recommendations, such as those outlined by the NIST cybersecurity framework.
- Show your involvement in information sharing groups, such as the FS-ISAC, and participation in CAPP exercises. (See the “ABA and Industry Events” section below for more information about the CAPP exercise.)
- Understand and be able to articulate how your institution assesses third-party risks and how the compromise of a third party could impact your institution's network.



## CyberSecurity Assessments ?

The CyberSecurity Assessment does not impose new expectations for institutions, nor will it result in any new examination rating.

**NO new expectations – NO new Rating!**

## CyberSecurity Definition:

- The activity or process, ability or capability, or state whereby **information** and **communications systems** and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation



<http://niccs.us-cert.gov/glossary#cybersecurity>

## Extended Cybersecurity Definition:

Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass(ing) the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations , information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.



<http://niccs.us-cert.gov/glossary#cybersecurity>

COMPLIANT CONSISTENT CONFIDENT

## Cyberspace Definition:

- The **interdependent network of information technology infrastructures**, that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.



<http://niccs.us-cert.gov/glossary#cybersecurity>

## What Is Security and Resilience?

### Security

- Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience defines security as reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.
- Examples of security measures: badge entry at doors, using antivirus software, fencing around buildings, locking computer screens.

<http://www.dhs.gov/what-security-and-resilience>

## What Is Security and Resilience?

### Resilience

- PPD-21 defines resilience as the ability to **prepare** for and **adapt** to changing conditions, and **withstand** and **recover** rapidly from disruptions.

Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.



<http://www.dhs.gov/what-security-and-resilience>

PPD = Presidential Policy Directive

Examples of resilience measures: developing a business continuity plan, having a generator for back-up power, using building materials that are more durable.

## Three strategic imperatives:

1. Refine and clarify functional relationships to advance the national unity of effort to **strengthen critical infrastructure security and resilience**;
2. Enable effective **information exchange** by identifying baseline data and systems requirements; and
3. Implement an integration and analysis function to **inform planning and operations decisions** regarding critical infrastructure.

shall drive the Federal approach to strengthen critical infrastructure security and resilience:

## Department of Homeland Security

Homeland Security wants corporate board of directors more involved in cyber-security

- New CyberRisk Guide targeted to Corporate Directors - RISK GUIDE

<http://www.nacdonline.org/AboutUs/NACDInTheNews.cfm?ItemNumber=10705>

**NACD = National Association of Corporate Directors**

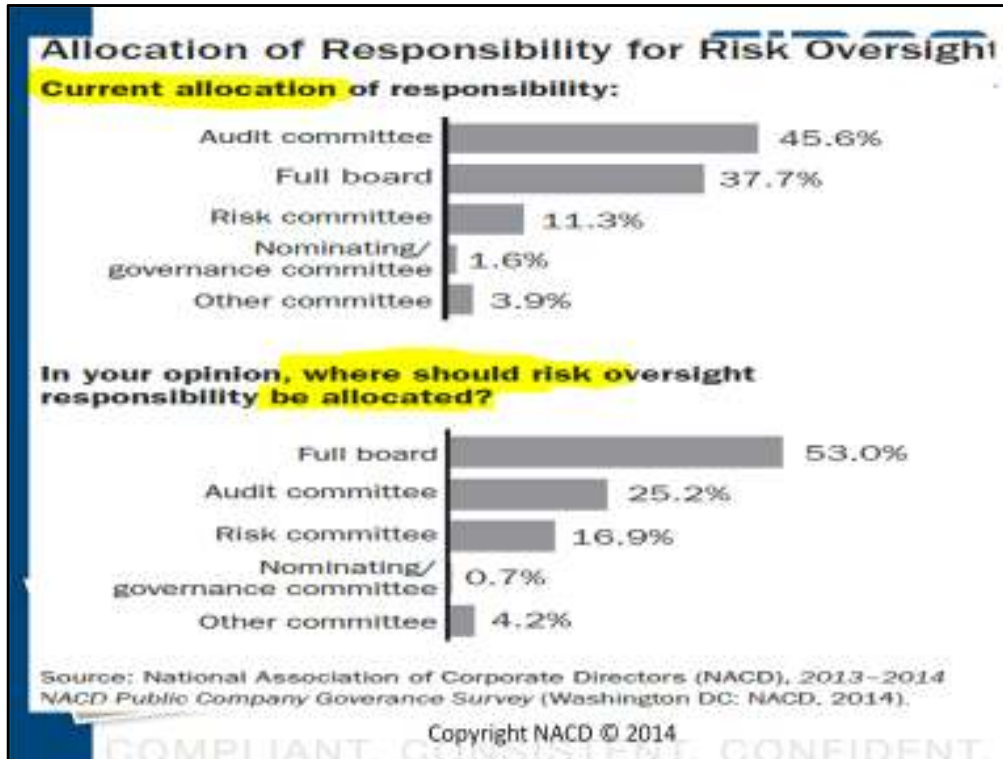
Copyright NACD © 2014



- **Principle #1**

Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

Copyright NACD © 2014



While including cybersecurity as a stand-alone item on board and/or committee meeting agendas is certainly a recommended practice, the issue should also be integrated into full-board discussions involving new business plans and product offerings, (M&A), new market entry, deployment of new technologies, major capital investment decisions such as facility expansions or IT system upgrades, and the like.

## NACD Oversight

*These are likely different than you've been used to!*

Since cyber risks and threats can change quickly, **committees with designated responsibility for risk oversight**—and for oversight of cyber-related risks in particular **Should receive briefings on at least a quarterly basis.**

The **full board** should be **briefed at least semiannually**, or as situations warrant.

Copyright NACD © 2014

- **Principle #2**

Directors should understand the **legal implications of cyber risks** as they relate to their company's specific circumstances.

Copyright NACD © 2014

- **Principle #3**

Boards should have adequate access to **cybersecurity expertise**, and discussions about cyber-risk management should be given **regular and adequate time** on the **board meeting agenda**.

Copyright NACD © 2014

- **Principle #4**

Directors should set an **expectation** that management establish **an enterprise-wide cyber-risk management framework** with adequate staffing and budget.

Copyright NACD © 2014

Ultimately, as one director put it:  
“**CyberSecurity is a human issue.**”<sup>32</sup>  
The board’s role is to .....

Copyright NACD © 2014

## NACD Principles COMPLIANT. CONSISTENT. CONFIDENT.

..... bring its judgment to bear and **provide effective guidance** to management, in order to ensure the company's **CyberSecurity strategy** is appropriately designed and sufficiently **resilient** given its strategic imperatives and the **realities** of the business ecosystem in which it operates.

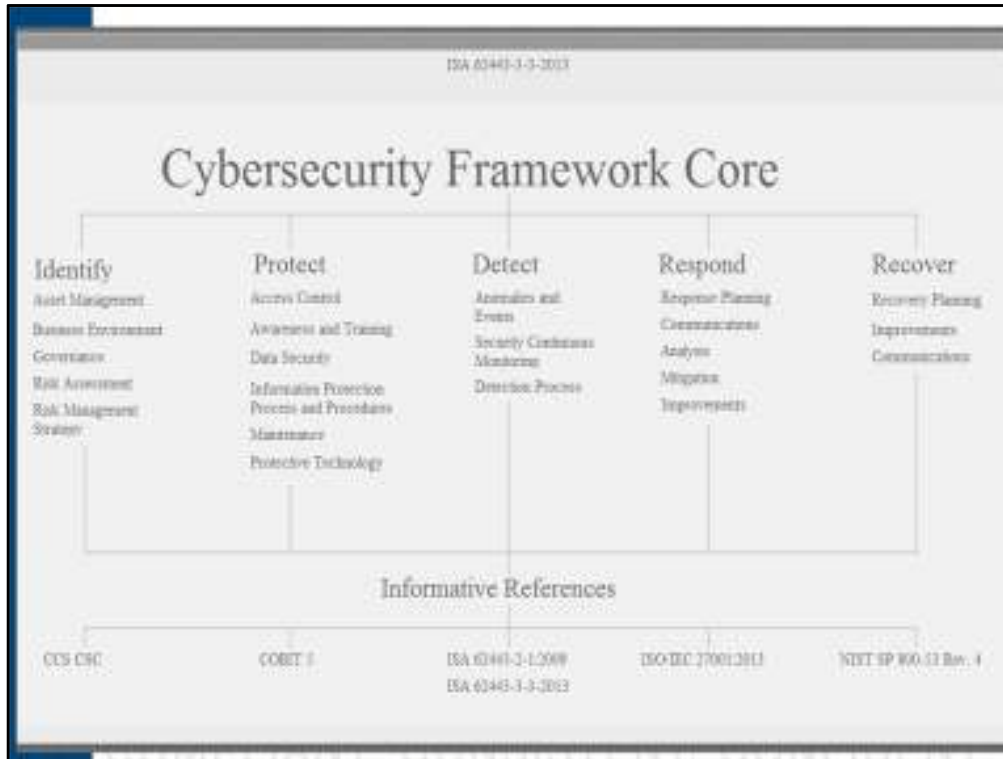
COMPLIANT. CONSISTENT. CONFIDENT.



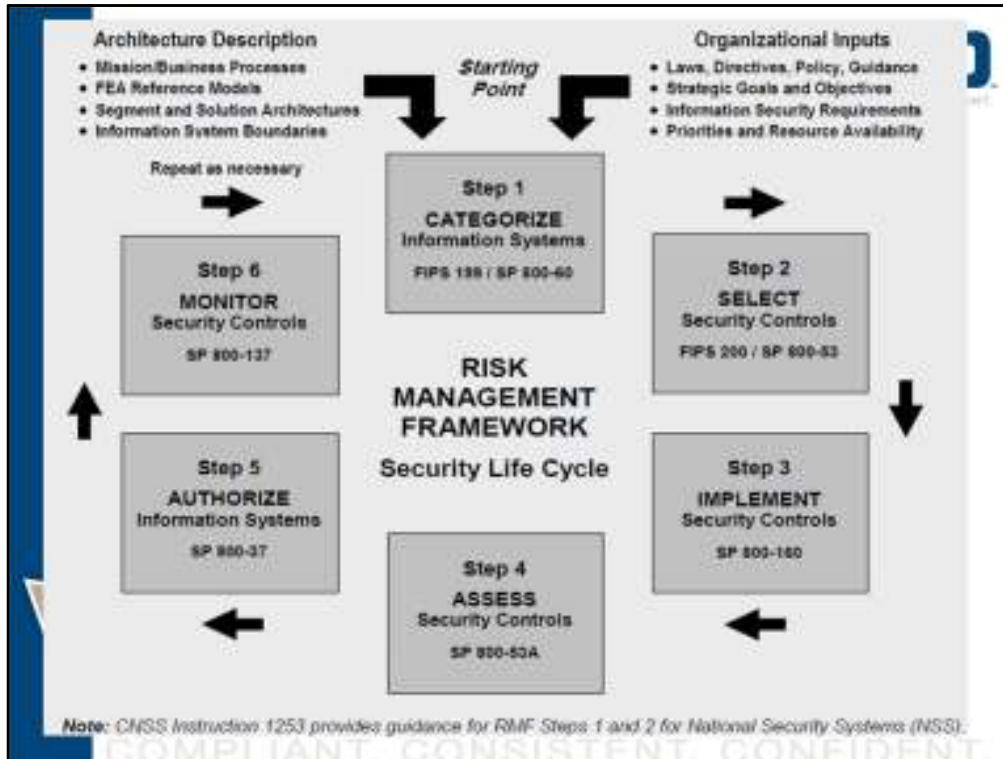
## What can we do?

- Deeper Layered and Exercised-Integrated Strategy for information security and Cyber..

Is there a way my bank can be prepared and self test ourselves to an industry standard (SP800-53) that likely will meet CyberSecurity Assessment Requirements?



The released framework is based on NIST SP800-53 for controls and the following categories were identified as the key components in a cybersecurity framework. Most organizations will find they are doing pretty well in probably 3 of the 5 with Detect and Respond being the least likely areas where high quality of user/computer activity monitoring and intrusion detection is performed. Too often event management tools are chosen and managed by the same people that need to be monitored, privileged users.



# Control Selection Guidance

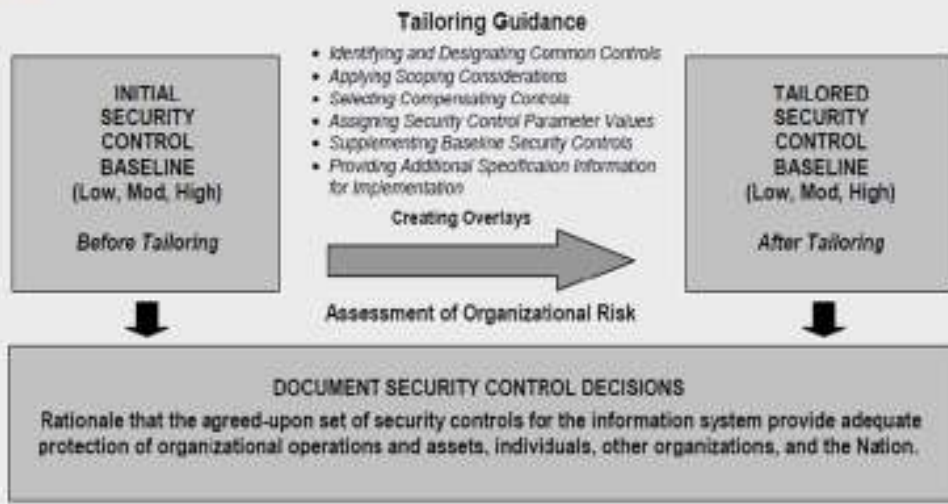


Figure 3: Security Control Selection Process

COMPLIANT. CONSISTENT. CONFIDENT.

## Would you like to Self Assess?

- Compare your Bank to NIST SP800-53 Rev4, and;
- Report to the Board your perceived security assurance level and identify areas of weakness.
- Receive Guidance, Budget, Approval and maybe just Risk Acceptance.

## [SP800-53 CyberSecurity Evaluation Tool](#)

(Industrial Control Systems Cyber Emergency Response Team – Assessment to multiple NIST Standards.) <https://ics-cert.us-cert.gov/Assessments>

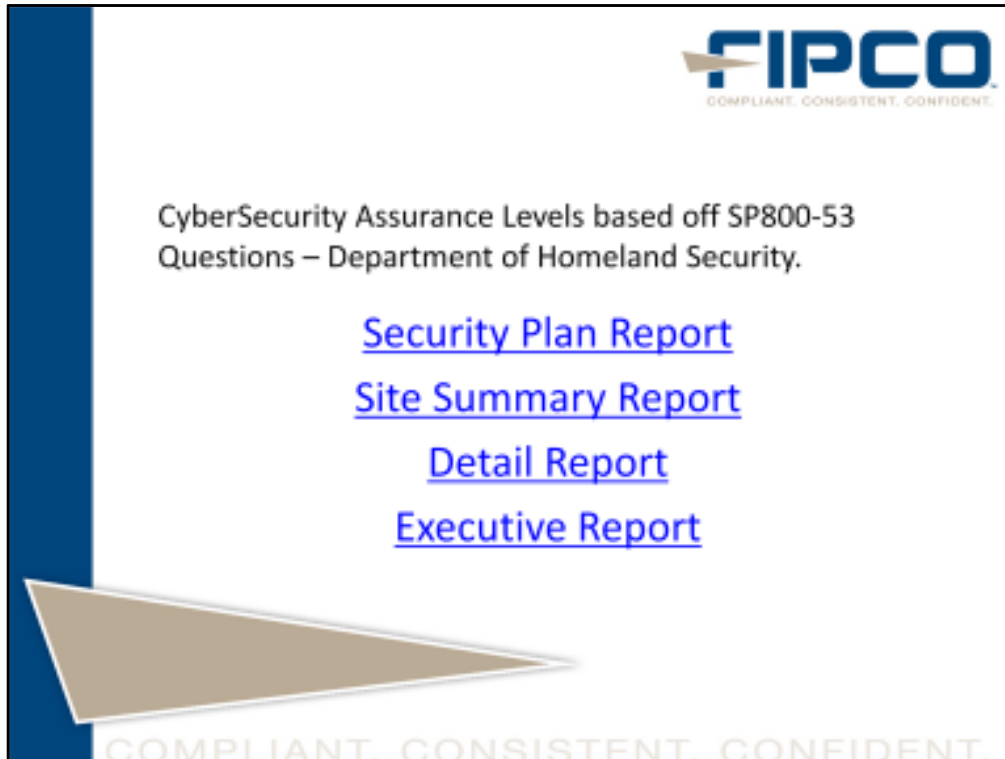
## [NIST Cybersecurity Framework \(CSF\)](#)

### [Reference Tool](#)

(Identify, Protect, Detect, Respond, Recover)

[http://www.nist.gov/cyberframework/csf\\_reference\\_tool.cfm](http://www.nist.gov/cyberframework/csf_reference_tool.cfm)

The CSF I find confusing and does not really offer much to assess your organization.



These are the series of reports available after responding to the set of questions in the CSET tool.

## Resources



### Securities Industry and Financial Markets Association (SIFMA) – Small Firms CyberSecurity Guidance

- <http://www.sifma.org/issues/operations-and-technology/cybersecurity/overview/>

### Cyber-Risk Oversight Handbook

- <http://www.nacdonline.org/Cyber>

### SEC - Office of Compliance Inspections and Examinations (OCIE) CyberSecurity Exam checklist & questions

- <http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf>

COMPLIANT. CONSISTENT. CONFIDENT.



## Additional Resources

- <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>
- <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>
- <http://www.dhs.gov/sites/default/files/publications/EO-PPD%20Fact%20Sheet%2012March13.pdf>
- <http://www.osfi-bsif.gc.ca/Eng/fi-if/in-ai/Pages/cbrsk.aspx>
- <http://niccs.us-cert.gov/glossary#cybersecurity>
- [http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800-53r4\\_summary.pdf](http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800-53r4_summary.pdf)

**Questions?**



Ken Shaurette, CISSP, CISA, CISM, CRISC, IAM  
FIPCO - Director IT Services  
kshaurette@fipco.com  
608-441-1251

COMPLIANT. CONSISTENT. CONFIDENT.