Financial Regulation & Cybersecurity

New York State CyberSecurity Requirements for Banks: Groundbreaking or More of the Same?

"He who defends everything defends nothing."

Fredrick the Great

Draft Agenda

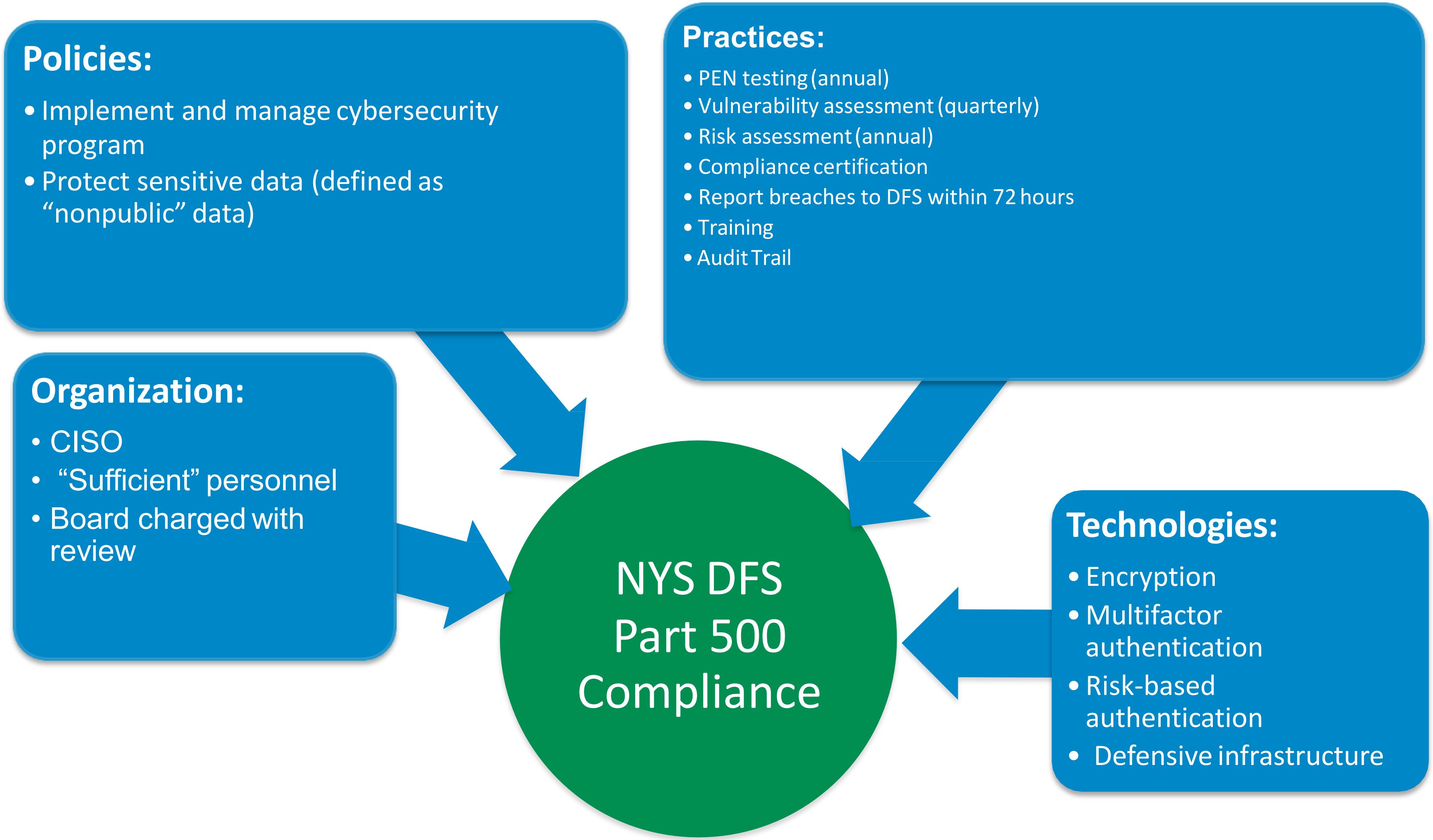
About NYS DFS Part 500

- Key Components
- Fundamental Principles
- Gaps and Challenges
- Next Steps

About NSF DFS Part 500

What it Is	• **Proposed regulation** defining requirements for cybersecurity • **Includes proscriptive requirements** for specific technologies, organization, practices, and policies
Who It Applies To	• **NY State financial entities** operating under a license, registration, etc. under banking, insurance, finance laws • Certain size-based exceptions apply
Key Milestones	• **Jan 1, 2017:** Takes effect • **Jan 15, 2018:** Compliance Required
Why You Should Care	• **Covered entities:** Compliance is required • **Other enterprises:** Other states, industries watching closely as template for regulation

NYS DFS Part 500 Key Components



Policies:

- Implement and manage cybersecurity program
- Protect sensitive data (defined as “nonpublic” data)

Practices:

- PEN testing (annual)
- Vulnerability assessment (quarterly)
- Risk assessment (annual)
- Compliance certification
- Report breaches to DFS within 72 hours
- Training
- Audit Trail

Organization:

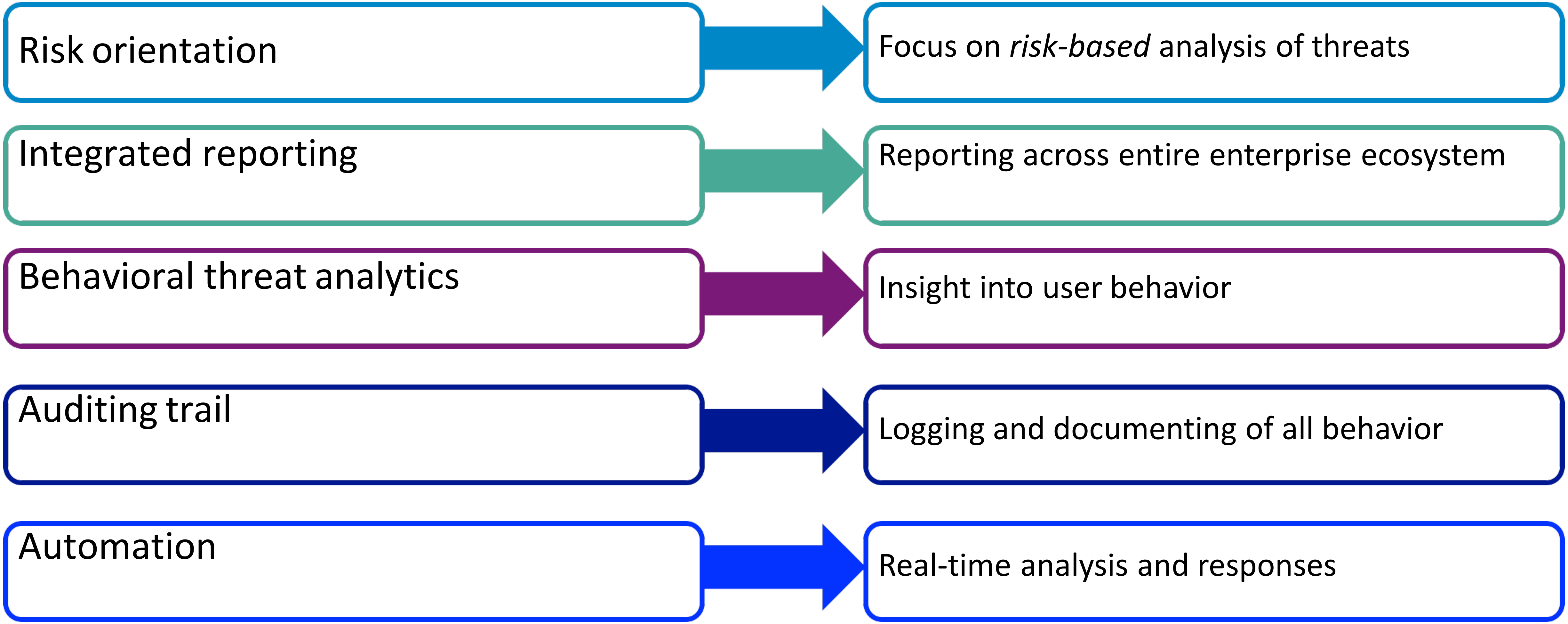
- CISO
- “Sufficient” personnel
- Board charged with review

NYS DFS Part 500 Compliance

Technologies:

- Encryption
- Multifactor authentication
- Risk-based authentication
- Defensive infrastructure

NYS DFS Part 500 Fundamental Principles



Risk orientation → Focus on *risk-based* analysis of threats

Integrated reporting → Reporting across entire enterprise ecosystem

Behavioral threat analytics → Insight into user behavior

Auditing trail → Logging and documenting of all behavior

Automation → Real-time analysis and responses

Part 500 Gaps and Challenges

- Prescribes technologies with unclear definitions
  - (“risk-based authentication”… “defensive infrastructure”)
- Potentially disruptive definition of non-public information
- Ambiguously defined assessments
- Lacks architecture, roadmap requirements
- Ambiguous requirements for staffing (no clarity onwhat constitutes “appropriate” levels)
- Does not explicitly address cloudsecurity
- Does not address roles of alternaterisk-remediation strategies (eg cybersecurity)

Top financial services issues of 2017

1. **Artificial intelligence** now drives the way leading firms provide everything from customer service to investment advice.

2. **Blockchain,** with its ability to store information data on distributed ledgers without a central clearinghouse, could upend a variety of businesses.

3.For decades, American firms looked to the United Kingdom as the gateway to Europe, but **Brexit** could change this.

4.Financial institutions face competition from nontraditional market players with skills, funding, and attitude. "**Fintech**"

5.In a prolonged low interest rate environment, many now look at cost containments one of the keys to survival.

6. Everything depends on robust cybersecurity to hold off threats that are coming from multiple directions.

7.The regulatory environment next year will likely be impacted from new appointments to the federal agencies and some targeted Dodd-Frank rollback by Congress, among other things.

8.And as the industry grapples with risk management culture, ethics, and trust, it often finds itself playing defense.

9.Digital labor, or robotic process automation, is helping firms automate things they couldn’t do before, without having to hire an army of developers.

10.Finally, we see firms in a search for new revenue opportunities, either organically, or through acquisitions. “ Disruption is Coming “ !