# Change is Coming
# GDPR – NYCRR 500 – PCI

**Scott Brod**

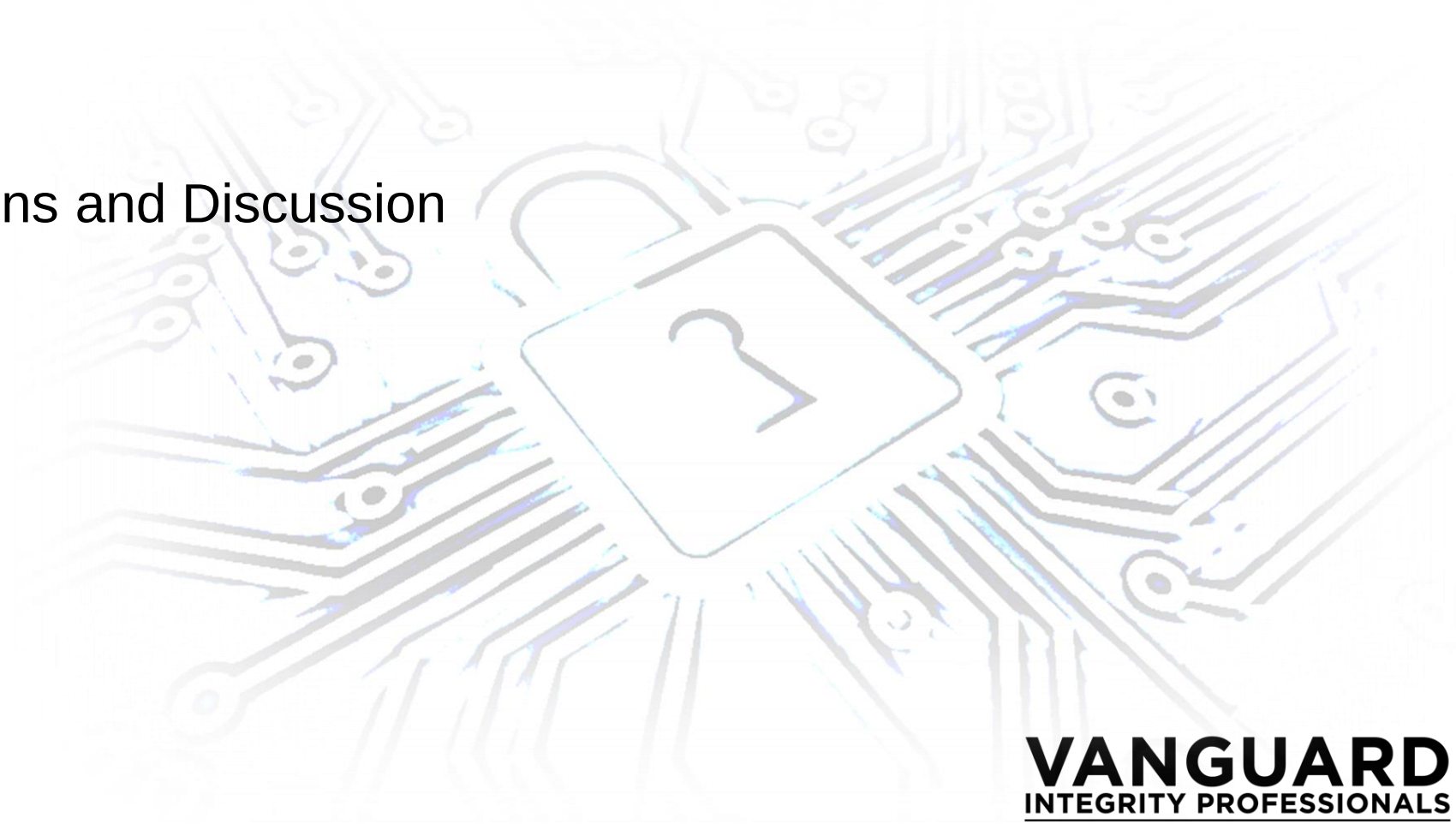
**Information Advisor for**

Vanguard Integrity Professionals

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# Agenda

- GDPR Overview
- NYCRR 500 Regulations and Discussion
- PCI, Quick Update



VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# What is GDPR

- The **General Data Protection Regulation** (**GDPR**) is a regulation intended to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

- The primary objectives of the GDPR are to give citizens and residents back control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.[1]

- It applies from 25 May 2018 after a two-year transition period and, unlike a directive, it does not require any enabling legislation to be passed by national governments

- It contains 11 Chapters and 99 Articles in the Actual Regulation.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# What is GDPR

The regulation applies if the data controller (organization that collects data from EU residents) or processor (organization that processes data on behalf of data controller e.g. cloud service providers) or the data subject (person) is based in the EU.

The Regulation also applies to organizations based outside the European Union if they collect or process personal data of EU residents.


VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# What is GDPR – Definitions

- **Data Controller** – The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- **Data Processor** - A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- **Consent** - Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

# GENERAL DATA PROTECTION REGULATION

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# General Data Protection Regulation

- **GDPR Compliance**
  - **Lead Supervisory Authority** – Responsible to investigate and resolve any problem identified, e.g. Information Commissioner in Country where problem occurred.
  - **Applies to Controllers & Processors Anywhere** – Performing activity on Personal Data of EU residents.
  - **Data Protection Officer** – Must be appointed by Controllers & Processors.
    - Contractually bound to the Data Controller.
    - Cannot process Personal Data for its own purposes.
    - Also responsible for GDPR Compliance requirements.
  - **Data Breach Notification** – To Supervisory Authority within 72 hours of discovery of breach or “suspicion” of breach.

# General Data Protection Regulation

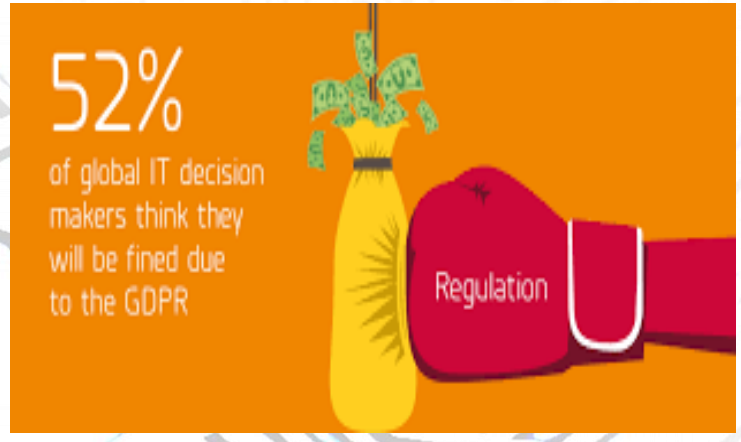
- **GDPR Compliance**
  - Collect and document affirmative consent from data subjects.
  - Provide evidence of consent for personal data already processed.
  - Mechanisms to erase personal data upon request by a data subject.
  - Documented Incident Management plans to notify supervisory authority within 72 hours and individuals without “undue delay”.

# General Data Protection Regulation

- **GDPR Compliance**
  - When Sharing Personal or Sensitive Data**:**
    - With whom is the Data shared?
    - What Data is being shared?
    - When is the Data being shared?
    - Why is the Data being shared?
    - Where is the Data being shared?
      - How is the Data being shared?
      - How much Data is being shared?
      - How is the Data being shared?
      - How is the Data being shared/ being protected by those with whom it is being shared?

# General Data Protection Regulation

- **GDPR Compliance**
  - Data Privacy Impact Assessment Process.
  - Audit trail of cybersecurity and resilience processes.
  - Monitor evolving cybersecurity attack methods.
  - Ensure legal counsel is aware of cyberattack activity.
  - Plan public relations response to a breach.




VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# GDPR = TEETH

- **GDPR Penalties**
  - Audit Authority.
  - Authority to stop aspects of Transacting business.
  - Fines.
    - **Up to 4% of Turnover (Revenue)**

IT HAS TEETH!


VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# GDPR – Expensive Mistakes

- All of the rest of the articles encompass a number of items including the supervisory authority, cooperation among supervisory authorities, the establishment and responsibilities of the power of the authorities and other legal matters including the most important:

- Fines can be depending on the provision anywhere up to 2% of the total worldwide annual turnover of the preceding financial year or $10,000,000 Euro (which ever is greater) or 4% and $20,000,000 Euro (whichever is greater).

# GDPR 6 PRINCIPLES + ARTICLE 9

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# GDPR – 6 Principles of Processing Personal Data

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject.

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

2. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss destruction or damage, using appropriate technical or organizational measures.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

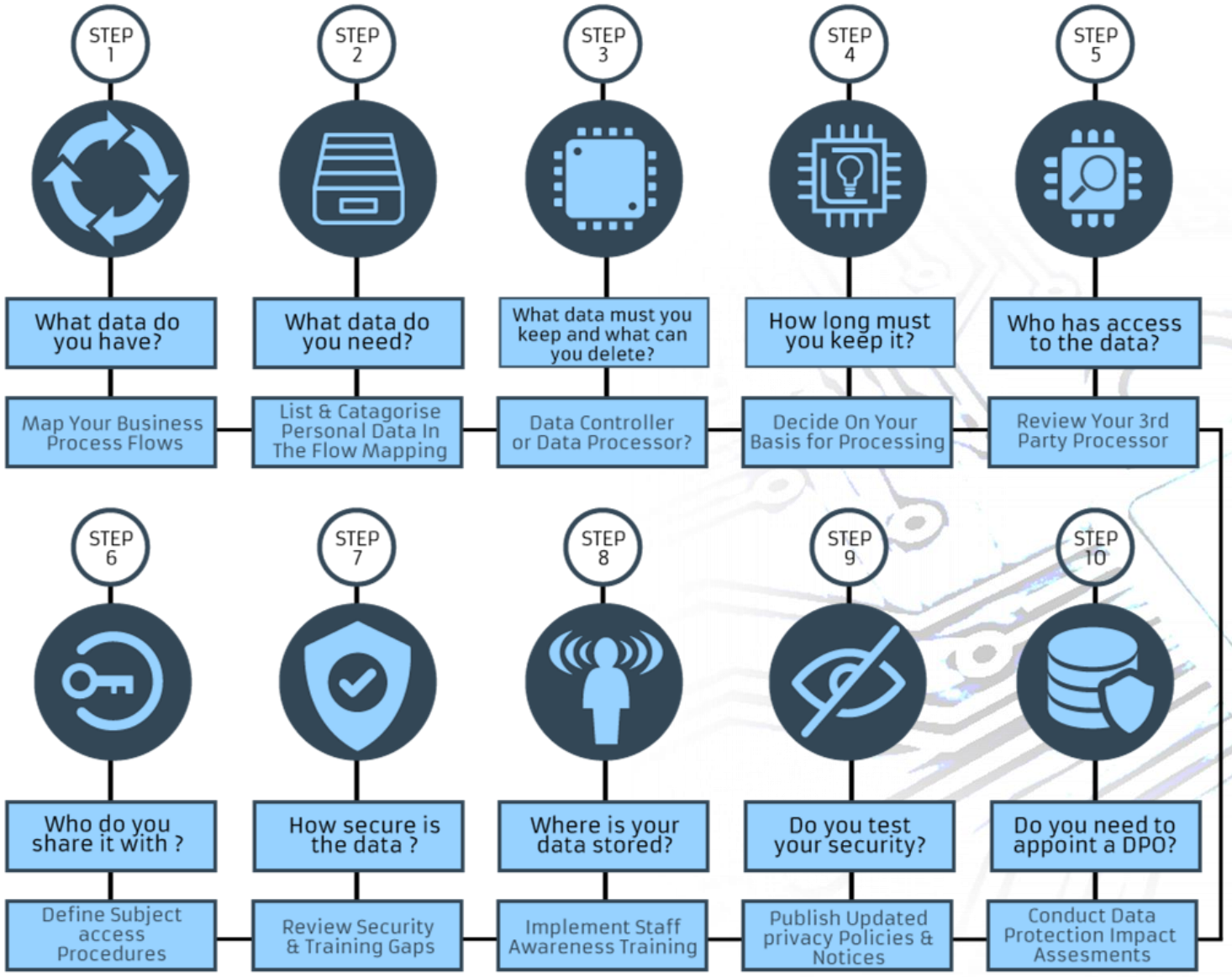
# GDPR – Article 9

**Processing of personal data revealing any of the following is Prohibited in Article 9**

1. Revealing racial or ethnic origin
2. Political opinions
3. Religious or philosophical beliefs
4. Trade union membership
5. The processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
6. Data concerning health
7. Data concerning a natural person's sex life or sexual orientation

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# GDPR Compliance Steps




VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

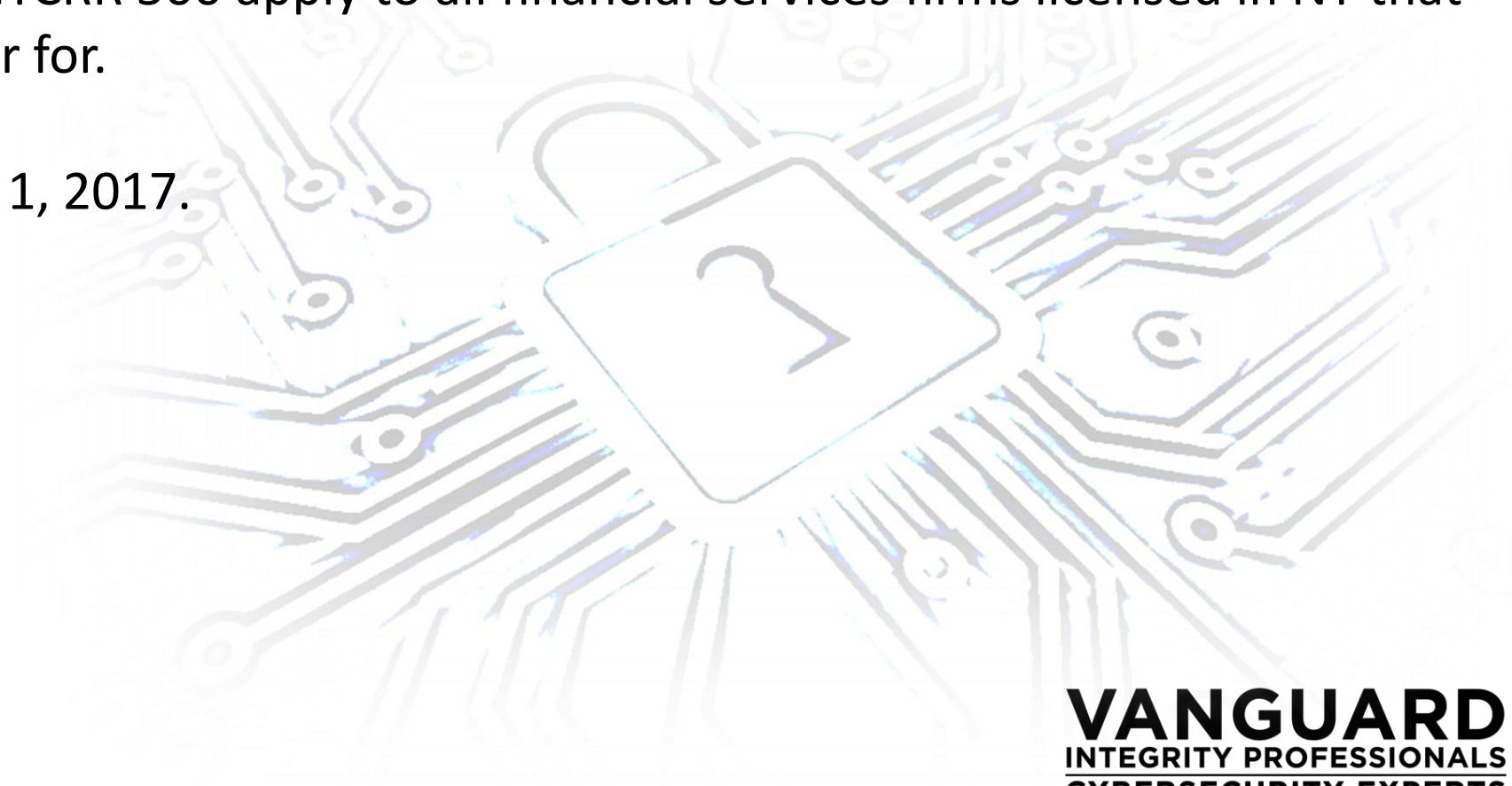
# 23 NYCRR 500 REVIEW

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# What is 23 NYCRR 500 ?

- In Sept 2016, NY State Department of Financial Services (DFS) under Governor Andrew Cuomo, announced a sweeping set of regulations to address growing cyber threats. These regulations known as 23 NYCRR 500 apply to all financial services firms licensed in NY that DFS serves as the regulator for.

- Most of it effective March 1, 2017.



VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# What is 23 NYCRR 500 ?

**In summary, the Regulation requires:**

1. The Establishment of a Cybersecurity Program.
2. The Adoption of a Cybersecurity Policy.
3. The Appointment of a CISO.
4. More stringent oversight of 3rd parties that have access to information systems and ‘nonpublic’ information.
5. Dictates Cybersecurity program elements.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# What is 23 NYCRR 500 ?

**The Cybersecurity Program (Section 500.02)**

- Each entity must have a cybersecurity program designed to protect, the confidentiality, integrity and availability of their information systems and it must be based on their Risk Assessment.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# What is 23 NYCRR 500 ?

**The Cybersecurity Policy (Section 500.03)**

- Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# 23 NYCRR 500 Compliance Checklist


VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# NY 500 REQUIRED CYBERSECURITY PROGRAM ELEMENTS

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# NYCRR 500 Required Cybersecurity Program Elements

**CISO and CISO reporting (Section 500.4)**

- Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy.

- The CISO of each Covered Entity shall report in writing at least annually to the Covered Entity's board of directors or equivalent governing body…the Covered Entity's Cybersecurity program and material Cybersecurity risks.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# NYCRR 500 Required Cybersecurity Program Elements

**Pen Testing & Vulnerability Assessments (Section 500.5)**

- Annual Penetration Testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and

- Bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# NYCRR 500 Required Cybersecurity Program Elements

**Audit systems to log access (Section 500.6)**

- Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk  Assessment:

- Each Covered Entity shall maintain records, no fewer than 3 or 5 years depending on the section of data the log records cover.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# NYCRR 500 Required Cybersecurity Program Elements

**Access Privileges (Section 500.7)**

- Based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# NYCRR 500 Required Cybersecurity Program Elements

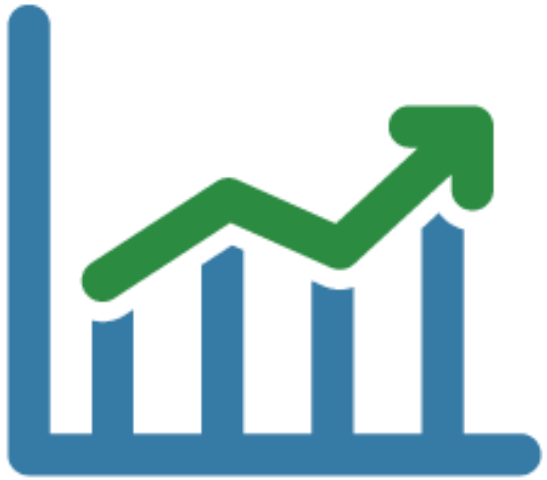
**Application Security (Section 500.8)**

Each Covered Entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment.

# NYCRR 500 Required Cybersecurity Program Elements

**Annual Risk Assessments of system integrity, adequacy of controls, and how risks will be mitigated (Section 500.9)**

Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program as required by this Part.



VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# NYCRR 500 Required Cybersecurity Program Elements

**Cybersecurity Personnel and Intelligence. (Section 500.10)**

Each Covered Entity shall:

1. utilize qualified cybersecurity personnel.
2. provide cybersecurity personnel with cybersecurity updates and training.
3. verify that key cybersecurity personnel take steps to maintain current knowledge.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# NYCRR 500 Required Cybersecurity Program Elements

**Third Party Provider Security Policy (Section 500.11)**

Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment.

Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# NYCRR 500 Required Cybersecurity Program Elements

**MFA for privileges users or remote access. (Section 500.12)**

- Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.

- Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.

# NYCRR 500 Required Cybersecurity Program Elements

**Limitations on Data Retention (Section 500.13)**

- As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# NYCRR 500 Required Cybersecurity Program Elements

**Training and Monitoring. (Section 500.14)**

As part of its cybersecurity program, each Covered Entity shall:

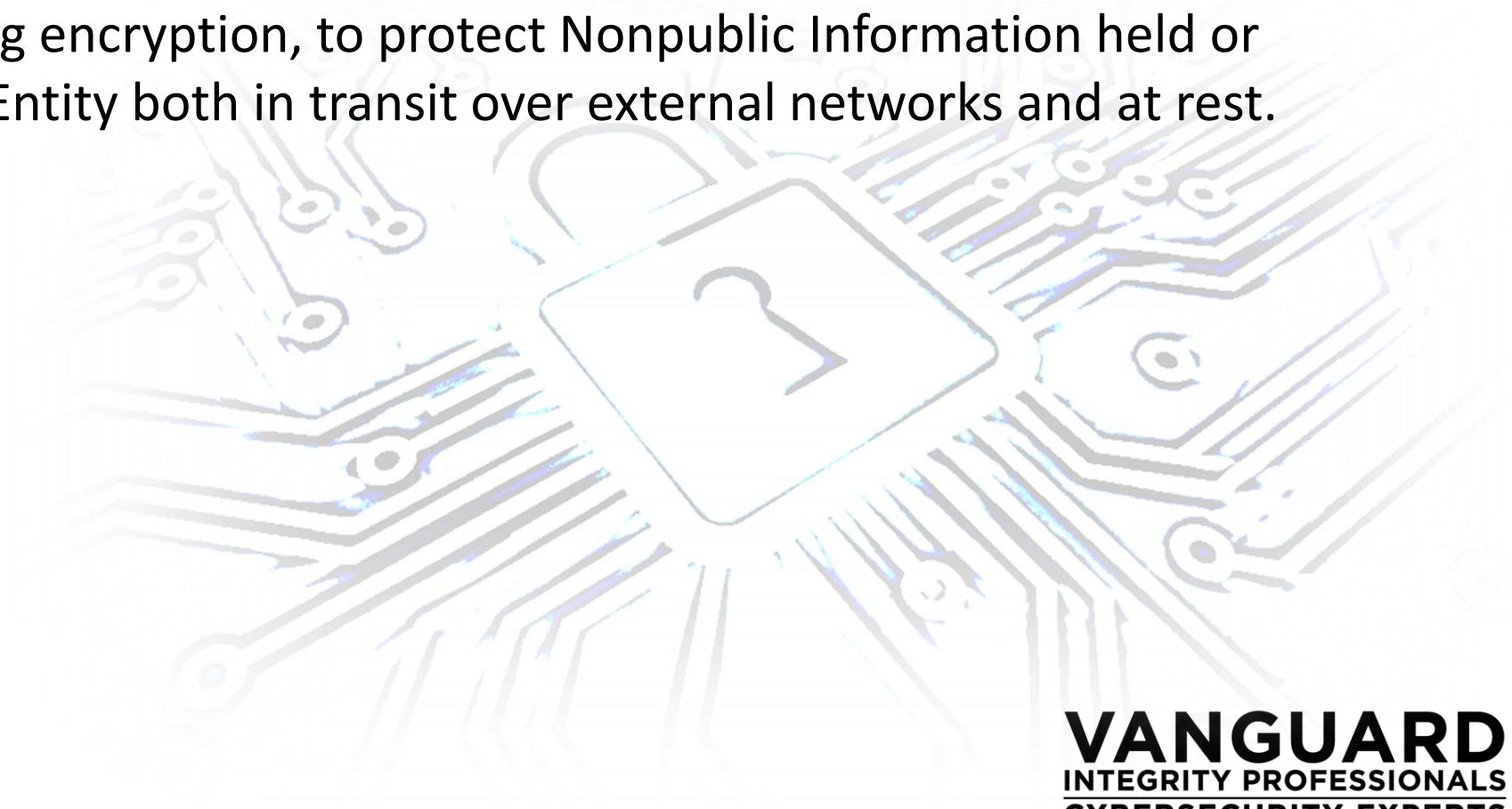
- Implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users.

- Provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

# NYCRR 500 Required Cybersecurity Program Elements

**Encryption of nonpublic information. (Section 500.15)**

As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.



VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# NYCRR 500 Required Cybersecurity Program Elements

**Incident Response Plan. (Section 500.16)**

As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# PCI 3.2 UPDATE

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# What is PCI DSS?

| PCI Data Security Standard - High Level Overview | | |
|---|---|---|
| **Build and Maintain a Secure Network and Systems** | 1 | Install and maintain a firewall configuration to protect cardholder data |
| | 2 | Do not use vendor-supplied defaults for system passwords and other security parameters |
| **Protect Cardholder Data** | 3 | Protect stored cardholder data |
| | 4 | Encrypt transmission of cardholder data across open, public networks |
| **Maintain a Vulnerability Management Program** | 5 | Protect all systems against malware and regularly update anti-virus software or programs |
| | 6 | Develop and maintain secure systems and applications |
| **Implement Strong Access Control Measures** | 7 | Restrict access to cardholder data by business need to know |
| | 8 | Identify and authenticate access to system components |
| | 9 | Restrict physical access to cardholder data |
| **Regularly Monitor and Test Networks** | 10 | Track and monitor all access to network resources and cardholder data |
| | 11 | Regularly test security systems and processes |
| **Maintain an Information Security Policy** | 12 | Maintain a policy that addresses information security for all personnel |

## About the PCI Security Standards Council:

- Global independent open body formed to develop, enhance, disseminate and assist with the understanding of security standards for payment account security.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# Common PCI DSS Requirements

**Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters**

| PCI DSS Requirements | Testing Procedures | Guidance |
|---|---|---|
| **2.2** Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.<br><br>Sources of industry-accepted system hardening standards may include, but are not limited to:<br>• Center for Internet Security (CIS)<br>• International Organization for Standardization (ISO)<br>• SysAdmin Audit Network Security (SANS) Institute<br>• National Institute of Standards Technology (NIST). | **2.2.a** Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards.<br><br>**2.2.b** Examine policies and interview personnel to verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.1.<br><br>**2.2.c** Examine policies and interview personnel to verify that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network.<br><br>**2.2.d** Verify that system configuration standards include the following procedures for all types of system components:<br>• Changing of all vendor-supplied defaults and elimination of unnecessary default accounts<br>• Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server<br>• Enabling only necessary services, protocols, daemons, etc., as required for the function of the system<br>• Implementing additional security features for any required services, protocols or daemons that are considered to be insecure<br>• Configuring system security parameters to prevent misuse<br>• Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. | There are known weaknesses with many operating systems, databases, and enterprise applications, and there are also known ways to configure these systems to fix security vulnerabilities. To help those that are not security experts, a number of security organizations have established system-hardening guidelines and recommendations, which advise how to correct these weaknesses.<br><br>Examples of sources for guidance on configuration standards include, but are not limited to: www.nist.gov, www.sans.org, and www.cisecurity.org, www.iso.org, and product vendors.<br><br>System configuration standards must be kept up to date to ensure that newly identified weaknesses are corrected prior to a system being installed on the network. |

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# PCI DSS 3.2 Update

- The extension of the SSL/early TLS dates to June 30, 2018 will be reinforced.
- Multi-factor authentication requirements for accessing the cardholder data environment, which were already in place for remote access scenarios, will be extended to include local access.
- There will be some new Appendices in the DSS, including one dedicated to SSL/early TLS and one that brings DESV requirements into the DSS.
- Rules around displaying card numbers will be modified to accommodate an upcoming change to card number standards.
- Service providers will undergo additional scrutiny of their change management processes, and penetration testing will be required.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# Key Dates for PCI DSS 3.2

- **April 2016:** PCI DSS 3.2, as well as all supporting documents and SAQs, will be released.

- **October 2016:** PCI DSS 3.1 will retire six months after the release of PCI DSS 3.2, and all assessments or SAQs taken after that time will need to use version 3.2. *This is significant for those with year-end annual assessment cycles.*

- **February 2018:** All new requirements within PCI DSS 3.2 will become effective. (Prior to that they will be considered “best practices.”)

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# TOP PCI CHALLENGES FOR Z/OS

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# Interpreting PCI DSS for z/OS

## What is a z/OS “System Component”

| 1st Systems Programmer | 2nd Systems Programmer | RACF Engineer | RACF Administrator |
|---|---|---|---|
| ✓ Master Catalog | ✓ SDSF | ✓ The RACF Database | ✓ Dataset Profiles |
| ✓ APF Authorized Datasets | ✓ Session Managers | ✓ Copies of the RACF database | ✓ General Resource Profiles |
| ✓ LINKLIB Datasets | ✓ SYS1.UADS Dataset | ✓ SETROPTS Settings | ✓ User ID Attributes |
| ✓ User Catalogs | ✓ WebSphere | ✓ RACF CDT | ✓ Group Connect Authorities |
| ✓ RACF Database | ✓ JES2 / JES3 | ✓ RACF Classes | ✓ Role Based Access |
| ✓ Parmlib Datasets | ✓ OMEGAMON | ✓ General Resource Profiles | Database Administrator |
| ✓ Multi-User Access Systems | ✓ WebSphere MQ | ✓ Encryption Keys | ✓ IMS Databases |
| ✓ z/OS Security Patches | ✓ DFSMS | ✓ Group Membership | ✓ DB2 Databases |
| ✓ System Proclibs | ✓ SVC’s | ✓ Privileged Userids | ✓ DB2 Table Trace |
| ✓ Started Tasks | ✓ CICS System Datasets | ✓ RACF Exits | ✓ Oracle Databases |
| ✓ SYS1.Parmlib | ✓ DB2 System Datasets | ✓ RACF Tables | ✓ RACF Classes for DB2 |
| ✓ SMF Log Files | ✓ IBM Comm Server | ✓ IRR Prefixed Utilities | ✓ IDMS |
| ✓ System Exits | ✓ Vendor Security Products | ✓ Logging Parameters | QSA & Compliance Officers |
| ✓ ICSF Encryption Keys | ✓ Magnetic Tape | ✓ | ✓ ? |

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# Identifying Not in Place Requirements

## What is a z/OS “System Component”

| Vanguard’s Top 10 z/OS Findings | | | |
|---|---|---|---|
| Rank | Description of Finding | Percent Occurrence of Finding | PCI Requirement |
| 1 | Excessive Number of User IDs with No Password Interval | 74% | 8.2.4 / 8.5 |
| 2 | Inappropriate Usage of z/OS UNIX Superuser Privilege UID(0) | 60% | 7.2.2 |
| 3 | Sensitive Data Set Profiles with UACC Greater than NONE | 54% | 7.2.2 / 7.2.3 |
| 4 | Critical Data Set Profiles with UACC Greater than READ | 54% | 7.2.2 / 7.2.3 |
| 5 | Started Task IDs are not Defined as PROTECTED IDs | 53% | 2.2.3 |
| 6 | Improper Use or Lack of UNIXPRIV Profiles | 52% | 7.2.2 |
| 7 | Excessive Access to SMF Data Sets | 44% | 7.2.2 / 7.2.3 |
| 8 | Excessive Access to APF Libraries | 42% | 7.2.2 |
| 9 | Excessive access to z/OS UNIX File System Data Sets | 42% | 7.2.2 |
| 10 | RACF Database is not Adequately Protected | 40% | 7.2.2 |

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# NVD and NCP

The NVD and NCP are a website cohosted by DHS and NIST that contain both checklists and vulnerability.

- **NVD --- The National Vulnerability Database** is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics. NVD supports the Information Security Automation Program (ISAP).https://nvd.nist.gov/

- **NCP --- is** the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications. https://nvd.nist.gov/ncp/repository

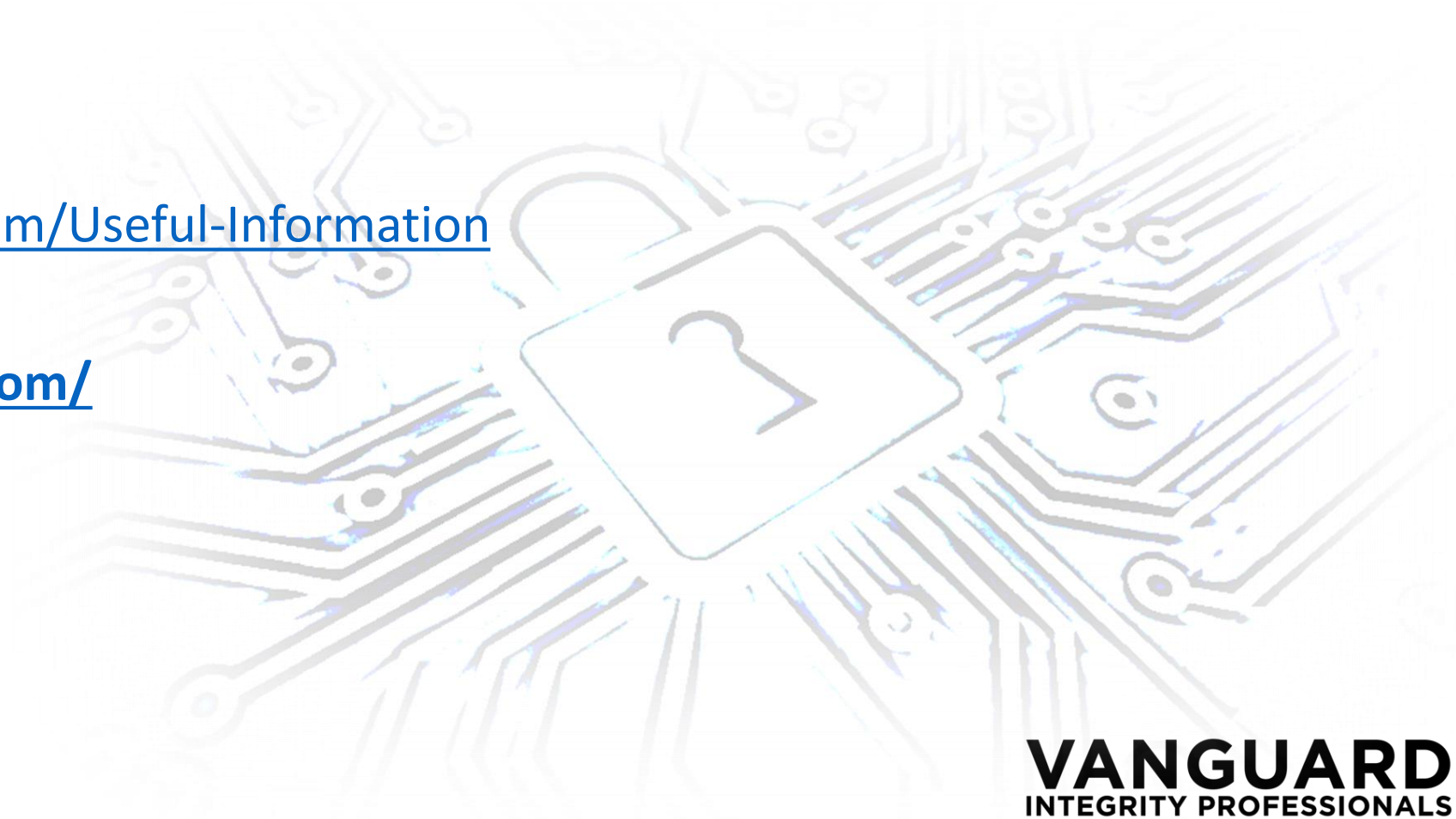
VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# Help and Questions

Here are some helpful Websites:

GDPR

- http://www.gdprwiki.com/Useful-Information
- **http://www.gdprwiki.com/**



VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# Help and Questions

Here are some helpful Websites:

## Requirements and Security Assessment Procedures

- https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
- https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

## PCI SSC Data Security Standards

- https://www.pcisecuritystandards.org/security_standards/index.php

# VANGUARD SECURITY COMPLIANCE 2018


VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# Help and Questions

**How to Contact Us**

Vanguard Integrity Professionals
6625 South Eastern Ave., Suite 100
Las Vegas, NV 89119-3930

Direct/International: (702) 794-0014
Toll Free: (877) 794-0014

**info@go2vanguard.com**

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS