Platzi

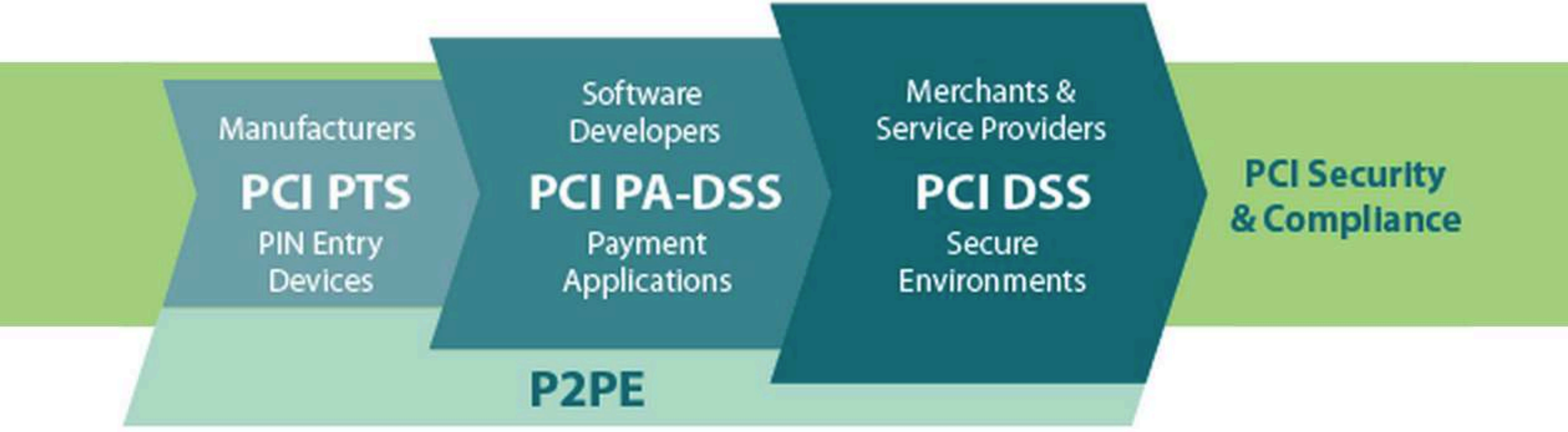
PCI Compliance

HIPAA Compliance

ISO 27001

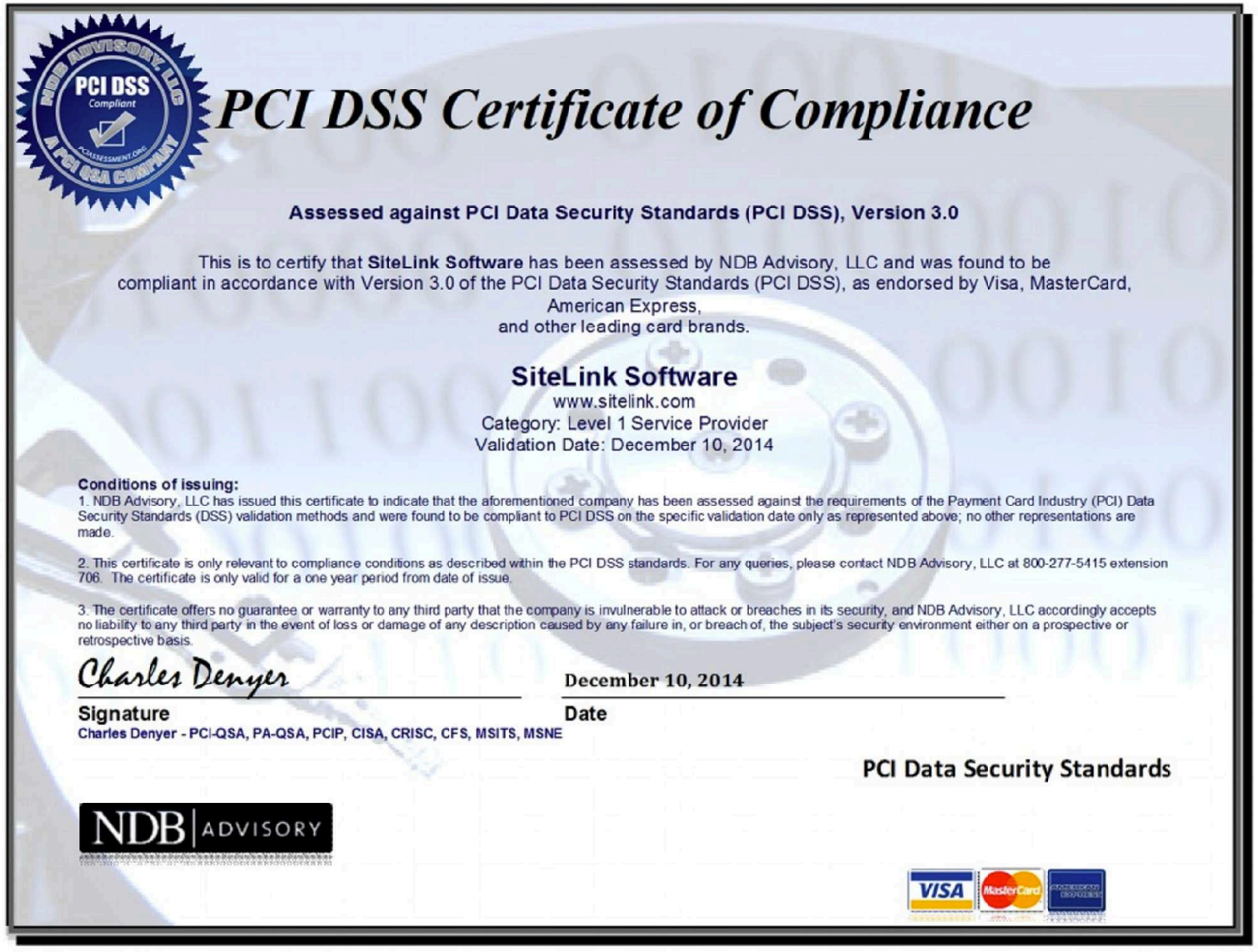
PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users

- Install & maintain a firewall to protect cardholder information
- Avoid use of vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Develop and maintain secure systems
- Use and regularly update anti-virus software and systems
- Encrypt transmission of cardholder data across open, public networks
- Restrict access to cardholder data on a need-to-know basis within the business
- Assign a unique ID to those who can access computers
- Restrict physical access to cardholder data
- Maintain a policy that addresses information security
- Test security systems on a regular basis
- Track and monitor all access to the network



PCI DSS Certificate of Compliance

Assessed against PCI Data Security Standards (PCI DSS), Version 3.0

This is to certify that **SiteLink Software** has been assessed by NDB Advisory, LLC and was found to be compliant in accordance with Version 3.0 of the PCI Data Security Standards (PCI DSS), as endorsed by Visa, MasterCard, American Express, and other leading card brands.

SiteLink Software
www.sitelink.com
Category: Level 1 Service Provider
Validation Date: December 10, 2014

Conditions of issuing:

1. NDB Advisory, LLC has issued this certificate to indicate that the aforementioned company has been assessed against the requirements of the Payment Card Industry (PCI) Data Security Standards (DSS) validation methods and were found to be compliant to PCI DSS on the specific validation date only as represented above; no other representations are made.

2. This certificate is only relevant to compliance conditions as described within the PCI DSS standards. For any queries, please contact NDB Advisory, LLC at 800-277-5415 extension 706. The certificate is only valid for a one year period from date of issue.

3. The certificate offers no guarantee or warranty to any third party that the company is invulnerable to attack or breaches in its security, and NDB Advisory, LLC accordingly accepts no liability to any third party in the event of loss or damage of any description caused by any failure in, or breach of, the subject's security environment either on a prospective or retrospective basis.

Charles Denyer — **Signature**
Charles Denyer - PCI-QSA, PA-QSA, PCIP, CISA, CRISC, CFS, MSITS, MSNE

December 10, 2014 — **Date**

PCI Data Security Standards

NDB | ADVISORY

6 STEP HIPAA COMPLIANCE CHECKLIST

1. **Map your data** and identify where your HIPAA protected files are (including cloud storage)
2. **Determine who has access** to HIPAA data, who should and implement a least privilege model
3. **Monitor all file access** to your personal health information data, this includes PHI and ePHI
4. **Set up alerts** for any HIPAA data that's accessed and new data put in a non-compliant repository
5. **Protect data** with physical and technical measures (locks, authentication, strong cyber-security)
6. **Monitor activity** on the perimeter and add threat models to your data security analytics

VARONIS

INFO PROTECTED BY HIPAA INCLUDES

- Names
- Birth, death or treatment dates
- Contact information
- Social Security numbers
- Medical record numbers
- Photographs
- Finger and voice prints
- Any other unique identifiers

VARONIS

STRUCTURE OF ISO 27001 2013 INFORMATION SECURITY MANAGEMENT STANDARD

ISMS stands for Information Security Management System.

- **4. CONTEXT**
  - 4.1 Understand your organization's context
  - 4.2 Define the expectations of interested parties
  - 4.3 Clarify scope of infosec management system
  - 4.4 Develop an infosec management system
- **5. LEADERSHIP**
  - 5.1 Provide leadership and show that you support ISMS
  - 5.2 Establish an appropriate information security policy
  - 5.3 Assign ISMS roles, responsibilities, and authorities
- **6. PLANNING**
  - 6.1 Formulate actions to address risks and opportunities
    - 6.1.1 Consider risks and opportunities when you plan your ISMS
    - 6.1.2 Establish an information security risk assessment process
    - 6.1.3 Develop an information security risk treatment process
  - 6.2 Set ISMS objectives and make plans to achieve them
- **7. SUPPORT**
  - 7.1 Support ISMS by providing resources
  - 7.2 Support ISMS by promoting competence
  - 7.3 Support ISMS by making people aware of duties
  - 7.4 Support ISMS by controlling ISMS communications
  - 7.5 Support ISMS by managing related information
    - 7.5.1 Include information and documents that the ISMS needs
    - 7.5.2 Manage the creation and modification of ISMS documents
    - 7.5.3 Control your organization's ISMS documents and records
- **8. OPERATIONS**
  - 8.1 Carry out planning and control your ISMS processes
  - 8.2 Conduct suitable information security risk assessments
  - 8.3 Implement information security risk treatment plans
- **9. EVALUATION**
  - 9.1 Monitor, measure, and analyze information security
  - 9.2 Set up audit program and use it to evaluate your ISMS
  - 9.3 Review your organization's ISMS at planned intervals
- **10. IMPROVEMENT**
  - 10.1 Identify nonconformities and take corrective action
  - 10.2 Improve information security management system

ISO 27001 CERTIFICATION PROCESS

RED = certification body

1 PREPARATION & DOCUMENTATION

Implement ISMS ensuring integration with existing Management Systems, processes and culture. Identify interested parties and applicable legislation; complete risk assessment complete risk treatment plan; develop Statement of Applicability. Identify accredited certification body

2 STAGE 1 AUDIT

Check of all documentation to confirm that all Management System elements completed. Understand how prepared you are for the Stage 2, and whether you understand the requirements of the standard. Confirm the scope of certification, and ensure plans in place for full implementation of your ISMS. Plan programme for Stage 2

3 ISMS IMPLEMENTATION

Ensure all controls implemented
Complete internal audit, including audit of all controls. Complete Management Review.
Maintain and review KPIs and Corrective Actions.
Maintain Continual Improvement

4 STAGE 2 AUDIT

Confirmation of implementation of ISMS, including:
- Interviews with senior management
- review of internal audits and audit trails
- Management Review
- compliance with legal duties
- check on controls
- KPIs
- staff awareness and competency

Plan programme for on-going visits

5 ISMS MAINTENANCE AND IMPROVEMENT

Ensure all controls continue to be implemented
Maintain risk-based internal audit programme, including audit of all controls.
Complete Management Reviews.
Maintain and review KPIs and Corrective Actions.
Maintain Continual Improvement

6 ON-GOING AUDITS

6- or 12-monthly checks to ensure ISMS effectively operated and maintained, with evidence of continual improvement.

Platzi