Digital Edge Compliance Services

Digital Edge's Compliance Solution for SOC 2 Consulting Services

Michael Petrov
Founder & CEO
Digital Edge Ventures
7 Teleport Drive
Staten Island, NY 10311

2019

About DIGITAL EDGE

Our mission is to develop and provide clients with a structured understanding of security frameworks, world class methodology and consulting services that deliver the best, most current policies and procedures for implementing, supporting and certifying Information Security Systems.

Established in 1996, Digital Edge specializes in…

- **Datacenter management and consulting service,**
- **Ensuring our clients achieve and maintain NIST, SOC, ISO, PCI, HIPAA,… certifications.**
- **Security Operation Center services.**
- **CyberSecurity assessments and penetration tests.**
- **Security Incident Investigations.**
- **Rapid Response Team for critical Security, System and Data related events.**
- **Delivering the required CyberSecurity framework unique to the client's business needs that complies with applicable laws and regulations.**

Digital Edge Services

Penetration Testing

External Scan
Internal Scan
Social Media Reconnaissance
Automatic and Manual
Penetration Test
Ethical Hacking
Reporting

Security Assessment

Penetration Testing
Laws and regulation analysis
Compliance Deficiencies Analysis
Architecture Review
Risk Analysis and Reporting
Business Continuity Analysis
Policy Analysis
Reporting

Building, Certifying and Supporting

Security Assessment
Framework selection (ISO, SOC2, NIST, etc.)
Development of Policies and Procedures
Staff Training
Technology review and integration
Management
Surveillance
Security Incident Response

Information Security System

Laws and regulation analysis
Gap Analysis
Risk Management
Controls Applicability and artifacts
Security Information and Event
Audit, CERTIFICATION
Security Operations

Digital Edge

Meet the Project Team

Michael Petrov, *CEO*

Danielle V. Johnsen,
VP, Compliance

Naum Lavnevich,
VP, Project Management

Demyd Maiornykov,
CyberSecurity Engineer

Digital Edge

Stability
Security
Efficiency
Compliance

- Access control
- Two-factor authentication
- Encryption

- Network/application firewalls
- Two-factor authentication
- Intrusion detection

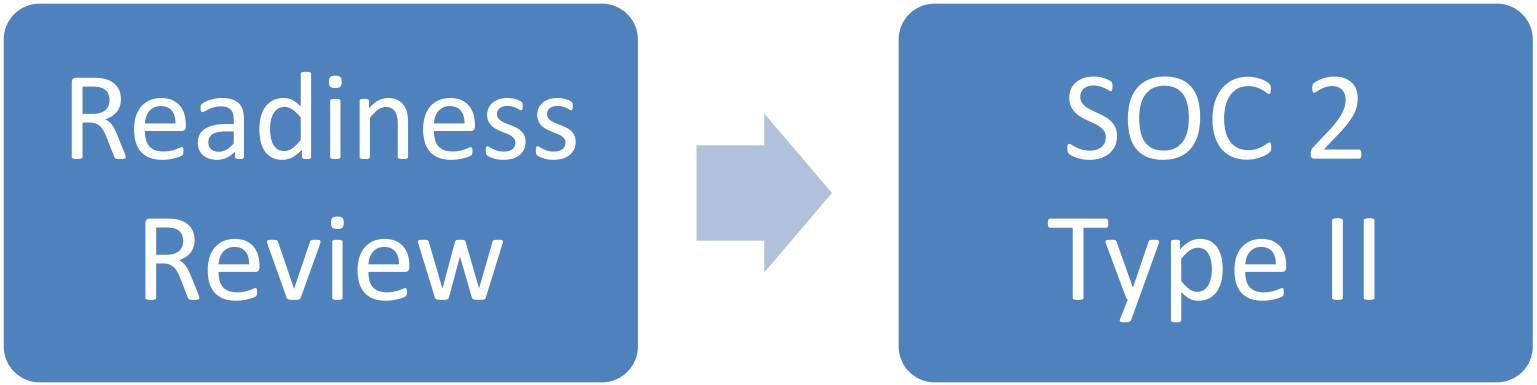
- Encryption
- Access controls
- Network/application firewalls

- Performance monitoring
- Disaster recovery
- Security incident handling

- Quality assurance
- Processing monitoring

7 Teleport Drive, Staten Island, NY 10311 800 714 5143

Our Approach

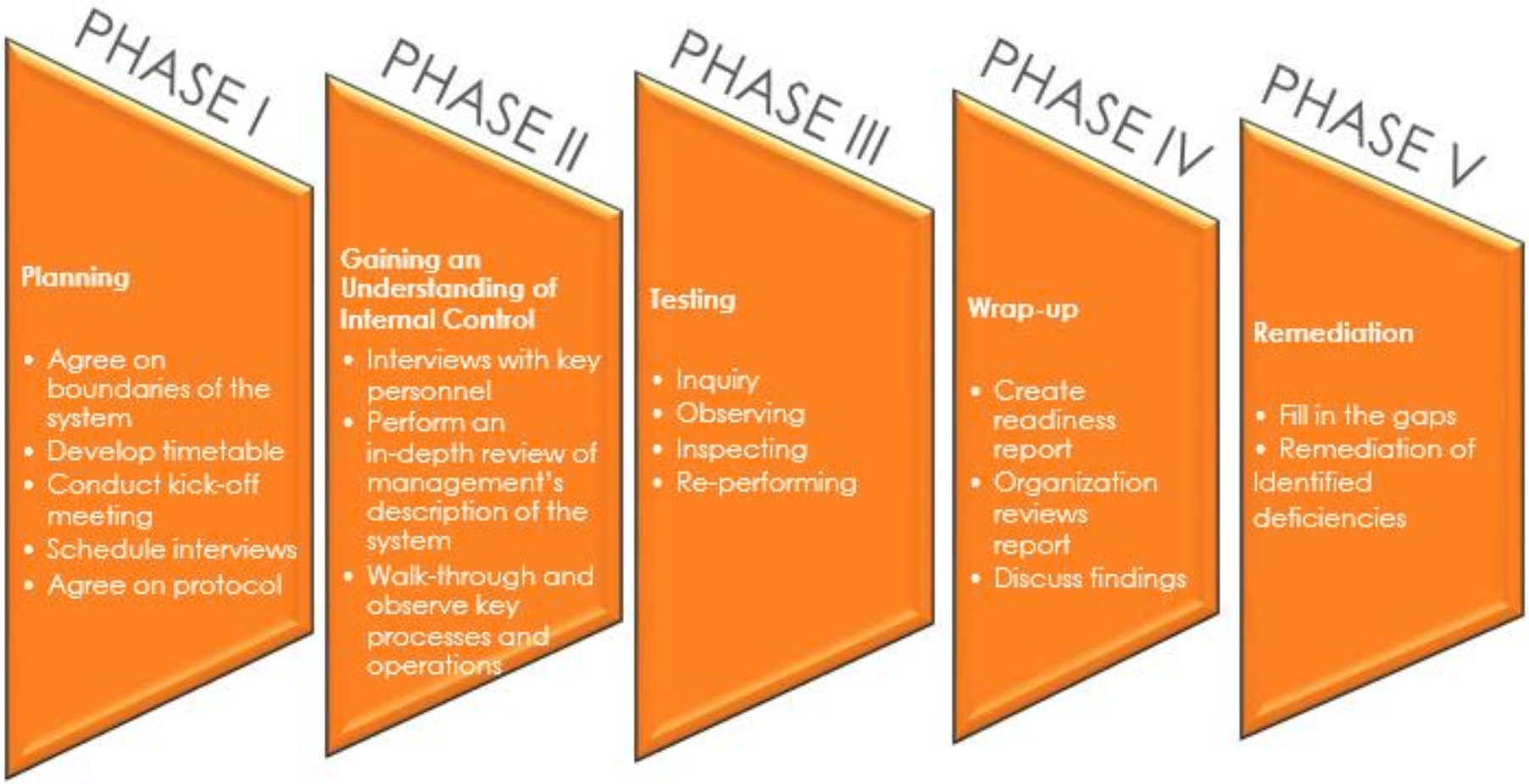


- Iterative Approach, ensures clients achieve a successful outcome, while meeting their customers' needs;
- Recommend a Readiness Review performed prior to a SOC 2 Type II examination;

Readiness Review

- Conducting a Readiness Review allows an organization to identify and remedy internal control deficiencies that would otherwise result in a modified opinion or as deficiencies;
- During the Readiness Review, we will assist the organization in preparing for the SOC 2 Examination;
- A Readiness Review differs from the Type II Examination in that the Readiness Review provides the results of the deficiencies in meeting the Trust Services Criteria in advance of the Examination and makes recommendations for remediation.

Readiness Review Phases



Phase I: Planning

Invest time to properly plan in order to set the proper pace and direction of the engagement.

Key objectives of this phase are:

- Discuss and Agree upon the scope and boundaries of the description of the system, including infrastructure, software, people, processes, and data,
- Agree upon a timetable and key milestones,
- Agree upon a status reporting protocol,
- Identify key stakeholders/senior executives subject to the examination,
- Hold a kick-off meeting with these executives and all key members of management to communicate the purpose, objectives, scope, timetable,

Phase I: Planning, continued

Key objectives of this phase are:

- Establish a communications protocol for correspondence, such as interview, document requests and handling of issues/findings,
- Explore and discuss any issues that could impact the nature, timing, and extent of our work performed, including significant changes expected to occur during the examination period that could impact the overall scope of the engagement or the control objectives and related control activities.

Phase II: Gain Understanding of Internal Controls

Our key objectives during this phase are to:

- Identify deficiencies in controls over the services subject to the examination,
- Describe the related risks.

During Phase II, we must….

- **understand the organization's internal controls over the services within the scope of the examination, including an overview of the criteria subject to the SOC 2**.
  - Hold a kick-off meeting with relevant senior executives,
  - Senior management completes a COSO top-level, self-assessment questionnaire,
  - Conduct separate interviews with each senior manager,

Phase II: Gain Understanding of Internal Controls

During Phase II, we must….continued

- The self-assessment questionnaire and individual interviews provide us with an understanding of the control environment, management's risk assessment process, and monitoring.
- Identify relevant IT and business managers responsible for Security related to the Trust Services Criteria;
- Conduct interviews in order to gain a detailed understanding; observe operations; inspect relevant documentation.

Phase III: Testing

Key objective….based on the security criteria, obtain reasonable assurances that in all material respects…

- the organization's control over the system relevant to security are suitably designed throughout the period to-be-determined,
- the description of the system relevant to security is fairly presented throughout the period to-be- determined
- the organization's controls relevant to security are operating effectively throughout the period to-be-determined

Phase III: Testing, *continued*

Testing Techniques	
Inquiry	Inquiries of appropriate personnel seeking relevant information or representations to obtain knowledge and additional information of the policy or procedure with their corroborating evidence.
Inspection	We will inspect samples of documents & records indicating performance of the controls. This testing includes, among other things: · Inspection of management reports; · Examinations of source documentation & authorizations to verify actions and occurrences; · Examination of documents or records for evidence of performance of a specific control;

Phase III: Testing, *continued*

Testing Techniques	
Inspection	· Inspection of systems' documentation, such as policies & procedures, operations manuals, flowcharts, and job descriptions; · Inspection of system configurations such as audit & logging enablement; system passwords; firewall rule sets; encryption methods, etc.
Observation	We will observe the application or existence of specific controls as represented.
Re-Performance	We will re-perform the control, or processing of the specific criteria, to help ensure the accuracy of its operation.

Phase IV: Wrap Up

Digital Edge's engagement team…

- completes our SOC 2 Readiness Review Report,
- provides a report including…
  - our opinion and the system description,
  - all workpapers our associates created,
  - senior auditors' review as the work progresses.

After the engagement team completes the report, a meeting will be held to discuss the findings and the remediation course of action.

Phase V: Remediation

Digital Edge will…

- work with client to fill in all applicable gaps,
- provide recommendations to remediate any identified deficiencies.

Questions and Answers