Ten key points from the SEC’s final Reg SCI

The Securities and Exchange Commission (SEC) published Regulation Systems Compliance and Integrity (Reg SCI) in the Federal Register on December 5th. Reg SCI is a comprehensive and wide-reaching new regulatory regime that requires certain market participants that are key to the functioning of the US securities market to “have robust technology controls and promptly take corrective action when problems arise.” Initially proposed in March 2013, Reg SCI replaces the voluntary Automated Review Policy (ARP) program, which has been in place since 1989. Reg SCI is about much more than making ARP mandatory; it adds more requirements as a response to the securities markets’ increasing dependence on technology and to increased concerns regarding cybersecurity.

Reg SCI requires entities subject to the final rule (SCI entities) to have comprehensive policies and procedures, “reasonably designed” for almost every aspect of establishing, operating, maintaining, and securing technology systems critical to promoting the maintenance of fair and orderly markets. The rule addresses five key areas of operational capability (i.e., capacity, integrity, resiliency, availability, and security) and requires SCI entities to be in compliance with most provisions by November 2015 (i.e., nine months after Reg SCI becomes effective in February). This does not leave a lot of time for the difficult task facing SCI entities of evaluating how they measure up to the rule’s requirements and how to address gaps.

1. **Compliance responsibility involves the entity’s senior management and board of directors:** The final rule requires that results of the mandated annual Reg SCI compliance review be submitted to the entity’s board and senior management (i.e., Chief Executive Officer, Chief Technology Officer, Chief Information Officer, General Counsel, and Chief Compliance Officer). After reviewing the report, senior management should note any material inaccuracy or omissions in the report. The report, along with any senior management responses, must then be submitted to the entity’s board and ultimately to the SEC.

2. **Non-ATS broker-dealers are exempt, for now:** Reg SCI applies to an estimated 44 entities, including self-regulatory organizations (e.g., securities exchanges and registered clearing agencies), alternative trading systems (ATS), including “dark pools,” plan processors, and exempt clearing agencies. However, despite active discussion earlier within the SEC to expand the rule’s scope to include non-ATS broker-dealers, the rule does not currently apply to these firms. Nevertheless, at the SEC meeting finalizing the rule, Chair White directed SEC staff to consider subjecting these broker-dealers to similar requirements in a future rulemaking.

---

1 See SEC Chair Mary Jo White’s statement from the meeting finalizing the rule.
3. **The final rule takes a risk-based approach:**
Reg SCI sets requirements for each system based on its operational criticality and on the level of risk the system’s malfunction would pose to maintaining both normal operations and fair and orderly markets. Three categories of systems are each assigned different regulatory requirements:

- **Critical SCI systems** are core to the functioning of the securities markets or have been identified as “single points of failure” and would have widespread and significant impact on the market if they failed. Examples include systems supporting clearance and settlement, provision of consolidated market data (i.e., SIPs), and IPOs.

- **SCI systems** directly support any of the six key functions considered to be central to the functioning of the US securities markets (i.e., trading, clearance and settlement, order routing, market data, market regulation, and market surveillance).

- **Indirect SCI systems** may be vulnerable to use as entry points to SCI systems and are subject only to the provisions of Reg SCI relating to security and intrusions. Notably, if SCI systems are appropriately protected, an SCI entity may have no systems in this category.

SCI entities may be expected to demonstrate how they categorized their systems, including providing their reviews of systems architecture and design.

4. **Development and testing systems are excluded, but not completely:** Typically over half of a firm’s systems are used for development and testing, so it is welcome relief to SCI entities that development and testing systems are now excluded from the definition of SCI systems. However, SCI entities will still be required to have policies and procedures for reviewing and keeping current systems development and testing methodologies. SCI entities should expect SEC examiners to review processes and systems relating to development and testing. At least to some extent, this brings development and testing systems back within the scope of Reg SCI, even if they have been deleted from the definition of SCI systems. Furthermore, development and testing systems that are not appropriately walled-off from production systems could be captured under the definition of indirect SCI systems (and therefore subject to the provisions of Reg SCI relating to security and intrusions).

5. **Although “Table A” has been removed, it has been replaced:** The Reg SCI proposal included a set of industry standards as guidance to SCI entities, collectively termed Table A. The final rule eliminates Table A and instead claims to give SCI entities more compliance flexibility by not being prescriptive in entities’ choice of industry standards. However, Table A has been recast and incorporated into the SEC staff guidance that identifies industry standards and was issued with the final rule. It is expected to evolve over time and is likely to be a benchmark against which an SCI entity’s processes, policies, and procedures will be measured.

6. **Industry- or sector-wide business continuity/disaster recovery (BC/DR) testing mandated annually:** Reg SCI requires an SCI entity (a) to conduct a BC/DR test at least once per year, (b) to designate participation by the entity’s members or participants, and (c) to coordinate this test on an industry- or sector-wide basis with other SCI entities. While Reg SCI is not prescriptive regarding the scope of the test, the scenarios, the duration of the testing, or the time the testing should be performed, the rule does require “functional and performance testing of the operation of BC/DR plans” which contemplates “next business day resumption of trading and two-hour resumption of critical SCI systems following a wide scale disruption.” SCI entities have until late 2016 to comply with the coordinated testing provision.

7. **The final rule provides some relief from reporting requirements:** The SEC’s risk-based approach in the final rule also reduces entities’ reporting burden for SCI events (i.e., systems disruptions, systems compliance issues, and systems intrusions). It eliminates the requirement to provide 30 days advanced notice of material changes and defines a new category of events (i.e., de minimis SCI events) that have no or little impact on the entity or on other market participants. De minimis SCI events are exempt from the reporting requirements applicable to all other events (i.e., reportable within 24 hours of detection), although SCI entities must keep a record of these events to be provided to the SEC upon request. SCI entities should not overlook de minimis SCI events, as trends or patterns of occurrences may cause regulatory concern.
8. **The scope of systems disruption has been narrowed to focus on operational continuity:** The proposal’s seven categories of system malfunctions that would constitute a systems disruption have been removed from the final rule. Instead, the final rule’s definition of systems disruption is based on whether the service has been halted or degraded in a manner that is outside of its “normal operations.” Certain events that would have been categorized as a systems disruption under the proposal (e.g., an SCI system experiencing an unplanned outage but transitioning seamlessly to backups and resuming normal operation) are no longer categorized as such under the final rule and would now be categorized as a de minimis SCI event. However, since the final rule does not define the term “normal operation,” SCI entities will need to clearly define the term for themselves.

9. **Prevention is better than cure:** The final rule introduces the new requirement that firms have policies and procedures in place for systems monitoring and a process for escalating identified issues. Consistent with the final rule’s risk-based approach, the requirement may be tailored to the relative criticality of a specific system – i.e., by devising more rigorous systems monitoring, policies, and procedures for more critical systems.

10. **SCI entities have work to do:**
- SCI entities should review their systems and determine which fall into the scope of critical SCI systems, SCI systems, and indirect SCI systems. This is a key step in determining what will need to be done to bring each system into compliance with Reg SCI by the deadline.
- SCI entities should initiate an assessment to identify any weaknesses in their policies and procedures, and to ensure that they are “reasonably designed” to achieve adequate standards of capacity, integrity, resiliency, availability, and security. SCI entities should compare current policies and procedures to industry standards and to evolving SEC staff guidance. Just because prior policies and procedures were deemed sufficient to meet ARP standards does not mean they will meet Reg SCI’s requirements.
- Beyond policies and procedures, SCI entities should review the design of their systems. As the final rule release states, an SCI entity “may also find it useful to conduct reviews of its software and systems architecture and design to assess whether they have flaws or dependencies that constitute structural risks that could pose a threat to SCI systems’ operational capabilities.”
- SCI entities should also track and manage operational and systems development performance. Referencing the adage, “you can’t manage what you can’t measure” and “if you can’t measure it, you can’t improve it,” we suggest that SCI entities revisit their scorecards and baseline their current operational and systems development capabilities (e.g., availability and capacity) in the context of Reg SCI.
For additional information about PwC's Financial Services Regulatory Practice and how we can help you, please contact:

**Dan Ryan**
Financial Services Advisory Leader
646 471 8488
daniel.ryan@us.pwc.com

**David Sapin**
Financial Services Regulatory Partner
646 471 8481
david.sapin@us.pwc.com

**Armen Meyer**
Director of Regulatory Strategy
646 531 4519
armen.meyer@us.pwc.com

**Christopher Pullano**
Financial Services Advisory Partner
646 471 2580
christopher.pullano@us.pwc.com

**Troy Paredes**
Senior Strategy & Policy Advisor
202 309 2850
troy.a.paredes@us.pwc.com

**Contributors:** Paul Chew, Andrew Papandreadis, William Pappas, Rachel Parker, Kevin Pilarski and Michael Savelloni.

To learn more about financial services regulation from your iPad or iPhone, click here to download PwC's new Regulatory Navigator App from the Apple App Store.

Follow us on Twitter @PwC_US_FinSrvcs