FAQ for Cyber Security Best Practices

Who is the DSOB?

The Data Security Oversight Board (DSOB) is a subset of SPARK Institute members focusing on data security standards amongst the record keeping industry. We currently have 38 members made up of both record keepers and plan consulting firms.

What are the 16 control objectives?

The 16 control objectives were derived from a list of over 1,300 questions submitted to member firms and then organized into overall control topics. These control topics include:

1. **Risk Assessment & Treatment,**
2. **Security Policy,**
3. **Organizational Security,**
4. **Asset Management,**
5. **Human Resources Security,**
6. **Physical & Environment Security,**
7. **Communications & Operations Management,**
8. **Access Control,**
9. **Information Systems Acquisition Development,**
10. **Compliance,**
11. **Incident & Event Communications Management,**
12. **Business Resiliency,**
13. **Mobile,**
14. **Cloud Security,**
15. **Software Application Security,**
16. **Encryption.**

Why is an outside audit required for compliance?

An independent outside audit brings an objective review & provides our clients with an appropriate level of assurance. In this way vendors can properly validate the robust nature of their cyber security systems and still provide assurances to clients and prospects through reporting on the objectives.

Why did SPARK feel another certification standard was required?

The intent of these standards is to establish a base of communication between record keepers and the public through the use of independent third-party audits of cyber security control objectives. The standards were developed to help record keepers communicate, to plan consultants, clients and prospects, the full capabilities of their cyber security systems.

Is this a one-time thing?

No- SPARK's Data Security Oversight Board is a permanent ongoing authority, with the responsibility to regularly review these standards and when necessary issue updates. So, within the first six months from the date of enactment of these new industry best practices the audit scope, the control objectives and appropriate frameworks will be reviewed. The control objectives and appropriate frameworks will be reviewed annually and updated as appropriate.

Will record keepers be required to comply with the spark best practices? What will happen if they don't?

No, record keepers can choose to adopt the standards, or not. However, with the buy in from most of the major consulting firms record keepers risk business opportunities for non-compliance.

Is there a time frame for record keepers to comply?

Since audit contracts need to be reviewed and adjusted we expect that over the next year most record keepers will comply with the new communications standards. Some record keepers may decide to quicken the process by self-certifying the 16 areas until they can get a third-party audit performed

These controls seen very high level and not very detailed; how much flexibility does each control have?

These 16 control areas actually require more detail that the newly established AICPA Cyber Attestation rules. SPARK's Industry Best Practices require record keepers to list all controls tested in each of the 16

control areas. This will allow clients, prospects and plan consultants more details than a simple pass/fail approach.

How should these best practices compare to other certifications...SOC2 or ISO...are they complementary or meant to substitute?

The SPARK Industry Best Practices are intended to be complementary to these other certifications. For example, a record keeper that conducts a SOC 2 audit would take an additional step of mapping the controls tested to the 16 control areas in the best practices. This mapping will allow clients and prospects to more easily compare vendors.