Scoping ISO 27001:2013 for success

measure twice. cut once.
Musa Wesutsa O’Wakwabi
Managing Director - Sentinel Africa

Musa has over 10 years work experience in IT, IT Security and Information Security Management. He is the cofounder and Managing Director of Sentinel Africa Consulting Limited.

His specialties include;
- Implementing and Auditing management system frameworks ISO 27001 and ISO 22301 for organisations such as Mumias Sugar, Safaricom Ltd, Airtel Ghana and East Africa Data Centre.
- IT and Information Security Process Improvement and Maturity
- Training and capacity building on ISO27001:2013 for numerous organisations

Contact Information

+254780572399
www.sentinelafrica.co.ke

musa.wesutsa@sentinelafrica.co.ke
twitter.com/@wesutsamusa
Some Project Management Statistics

**Small Teams**
- 28% Successful
- 67% Challenged
- 5% Failed

*The chart shows project resolution for teams with four to six members for calendar year 2012.*

**Resolution by Goal**
- 78% Successful
- 2% Failed
- 20% Challenged

*The chart shows the resolution of small projects with goals that match the corporate strategy.*

**Large Project Resolution in Banking**
- 44% Successful
- 7% Challenged
- 49% Failed

*The chart shows large project resolution in the banking industry, from 2003 to 2012. A large project is a project with more than $10 million in labor costs.*

**Small Project Resolution in Banking**
- 30% Successful
- 66% Challenged
- 4% Failed

*The chart shows small project resolution in the banking industry, from 2003 to 2012. A small project is a project with less than $1 million in labor cost.*

**Source:** The CHAOS Manifesto: The Standish Group International, Incorporated
10 steps to ISO/IEC 27001 Certification

1. Capacity Development
2. Perform a gap assessment
3. Scope the ISMS (Decide on certification body)
4. Establish ISMS policy/objectives
5. Conduct internal audit
6. Implement a document management system
7. Establish monitoring and measurement system
8. Assess the risks and develop operational controls
9. Conduct management review
10. Get certification audit conducted by a third party certification body
Must do's for a successful ISO 27001 implementation

- Appropriate Scoping
- Management Support
- Capacity Development
- Proper Consulting
- Right Certification Body
Certification Schema

Accreditation authorities
Ex: IAS (USA) – SCC (Canada) – UKAS (UK)
COFRAC (France) – BELAC (Belgium) – SAS (Switzerland)

Accredit

Certification bodies
Ex: PECB – SGS – Swiss TS

Certify organizations

Hire auditors

Certify auditors

Personnel certification bodies
Ex: PECB – BSI – Bureau Veritas

Certify training providers and trainers

Training organizations

Auditee

Audit the auditees

Auditors

Train the auditors
Scoping the ISMS

ISO 27001:2013 Clause 4.3 Determining the scope of the information security management system

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organization shall consider:

a) the external and internal issues referred to in 4.1;
b) the requirements referred to in 4.2; and
c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope shall be available as documented information.
In order for an organisation to comply with the requirements of ISO27001:2013 Clause 4.3 it must:
1. Define the boundaries of the management system
2. Justify and document exclusions to the scope
3. Document the ISMS Scope

SOURCE: PECB Certified ISO27001 Lead Implementer training manual
Scope determination – considerations on size

<table>
<thead>
<tr>
<th>Expansive Scope</th>
<th>Limited Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Ensures better utilization of effort</td>
<td>1. Ensures the definition of “crisp” boundaries</td>
</tr>
<tr>
<td>2. Usually has the involvement and contribution of the whole business and especially the senior leadership team</td>
<td>2. Easy adoption and buy-in to the change</td>
</tr>
<tr>
<td>3. The culture change occurs organisation-wide rather than piecemeal</td>
<td>3. Focuses only on the critical services, systems, people, sites, process</td>
</tr>
<tr>
<td>4. Gives the organisation a “quick win” enabling faster “ROI” and further support</td>
<td>5. Generally takes a shorter time to implement</td>
</tr>
</tbody>
</table>

![Pie chart comparison between small and large projects](chart.png)
Symptoms of poor scoping

- Project timelines extend
- Project outcome is not aligned to the strategy of the business
- Scope creep
- Confidence of project success is low
- Project is dependent on individuals – may not survive a change in personnel midway
Understand: ISMS Strategy Alignment

1. Business SWOT
2. List of I.Ps & Expectations
3. Understand regulatory and contractual obligations

Tailor: Reuse existing processes

1. List of SOPs
2. Engage people

Embed: Carry out Awareness

1. Training Gap Assessment
2. Define Awareness goals and objectives
3. Awareness Implementation Plan

The Sentinel Africa Way: Adapt don't Adopt
The Safaricom Ltd Case

The initial situation:
- The Company expressed a wish to go for ISO27001:2005
- This was driven by the CISO office.
- A Big Four consultant was contracted and the project begun
- Local staff were not involved

The outcome:
- Documentation was done (including Corporate Information Security Policy). The documents averaged 20 pages and had many required approvals.
- The scope document defined all critical business functions and systems of the Telco
- The CISO departed from the organisation
- The ISMS Steering Committee never met
- The Company was unable to go for Certification
The Safaricom Case contd...

The difference
- Focus on a defined scope
- The system in scope had Strategic alignment
- ISMS Steering committee was curved out of an existing Governance Body
- The implementation was done in Enterprise Risk Management
- The implementation team was made up of SPOCs in the organisation
- The documentation was designed for adequacy and suitability

The outcome
✓ The ISMS moves out of Project-mode and into BAU
✓ Safaricom Ltd gets ISO27001:2005 Certified in 2014!
✓ Safaricom has an ISMS whose scope was expanded on 2015 and recertified for ISO27001:2013
Conclusion – Think Big; Act Small

• **Value Estimation.** Creating accurate estimates for a project is difficult, but easier for small projects.

• **Optimal Team.** Think SEAL Team Six. S is for specialized for the project at hand. E is for exceptional. A is for assortment. Make sure the team has a diversity of experiences that fit the project. L is for love. The team should love what they do and be excited about the projects that they get assigned.

• **Managing Expectations.** It is much easier to set and manage expectations for small projects since the scope is kept to a minimum. Expectations in a project context might be the cost, time, or quality of an outcome (Certification).

• **The Butterfly Effect.** Small projects make a big impact. The reason they make a big impact is because they get completed, implemented, and used. Small projects also pave the way for more small projects that get implemented and used. They create an environment of success that breeds more success.

• **Continuous Improvement.** Small projects promote the continuous delivery of functionality and for our case Continual Improvement.

• **Motivation.** Small projects have built-in motivation. The greatest motivation of all time is the sense of accomplishment and belief that your efforts have meaning and value. Steppingstones provide a method to dole out incentives as the project progresses.
Q & A?