Agenda

• the organization structure of the project
• the work done so far (most in the area of definitions)
• rough timelines of the project
• short term activities
• how you can contribute
3.2. The Open Group

The Open Group will provide facilities for information sharing and conference calls. We can use their Webex facilities to host the meetings. There is also the possibility to use the Security Forum LinkedIn site and a Twitter account. Moreover, the expectation is that there are numerous members in the Security Forum and Architecture Forum who will have keen interest in this project once initiated.

The Open Group Security Forum
Director:
Jim Hietala
j.hietala@.opengroup.org

3.3. The SABSA Institute

The SABSA Institute will commit to this project and stimulate SABSA practitioners to contribute to and make use of the deliverables. The SABSA group on LinkedIn will also be used for this purpose. Soon as The SABSA Institute becomes fully operational, its web site and social media integration will also be available, and it will be a partner in the governance of the working group.

Chief Architect:
John Sherwood
john.sherwood@sabsa.org

3.4. The Open Security Architecture

The Open Security Architecture community, represented by Tobias Christen, is willing to pass on experience in security architecture.
Organization (2)

- Pascal de Koning - project chairman
- Chris Blunt - co-chair
- Jeff Primus - co-chair

>60 participants!
THE WORK DONE SO FAR
Working definition of a security service

A Security Service is a combination of security controls working in an integrated fashion to support business and customer services, to provide a specific level of service and business value.

A security service is a defined capacity, with a defined input and defined output. It is self-contained, repeatable and has clear ownership.

Security services are logical services. Services are specified independently of what physical mechanisms might be used to deliver them. A service can be a black-box. A consumer doesn’t need to know how it works internally, but just enough information in order to use it.

Security services may consist of sub-services. The view on this depends on the abstraction level of a given context. Common distinctions are enterprise-level services versus solution-level services.
The function of a catalogue

To give an idea of the function of the catalogue, we use a historic source from a librarian. Charles Ammi Cutter made the first explicit statement regarding the objectives of a bibliographic system in his Rules for a Printed Dictionary Catalog in 1876.

According to Cutter, those objectives were

1. to enable a person to find a book of which either (Identifying objective)
   - the author
   - the title
   - the subject
   - the category
   is known.

2. to show what the library has (Collocating objective)
   - by a given author
   - on a given subject
   - in a given kind of literature

3. to assist in the choice of a book (Evaluating objective)
   - as to its edition (bibliographically)
   - as to its character (literary or topical)
1.1. Vision

For security architects, the security services catalogue is a register that supports filling in the logical (aka functional) layer of the architecture with security controls. Unlike existing control frameworks that contain requirements, the security services catalogue describes security building blocks that actually deliver protection. This architecture approach enables smooth integration of information security in the enterprise architecture.

The standardized approach contributes to the professionalization of the security management organization and facilitates a more efficient and cost effective way of working. One of the main advantages of the Security Services Catalogue is that it is a common terminology and reference framework for the domain of security management allowing better cooperation between the parties concerned.
Project principles

• It’s not about the truth or being right, it’s about creating something that works
• The relationships between participants is an important deliverable too
• We use group wisdom
• We don’t aim for consensus
Trusted Architecture

key characteristics:
- traceability
- justification
- measurement

Services Catalogue links objectives to technique.
Conceptual services versus actual situation

Q1. How important is this security service?

Q2. Is this security service implemented? (sufficient / partly / not)

Q3. How exactly is it implemented?
Example:
Security Services Landscape

<table>
<thead>
<tr>
<th>Application</th>
<th>Security</th>
<th>Service Delivery</th>
<th>Service Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database management</td>
<td>Identity &amp; Access Mgt (IAM)</td>
<td>Incident Management</td>
<td>Service Development Process Model</td>
</tr>
<tr>
<td>Webserver management</td>
<td>Business Continuity Mgt (BCM)</td>
<td>Request Fulfilment</td>
<td>Project Management</td>
</tr>
<tr>
<td>Log Management</td>
<td>Security Management</td>
<td>Problem Management</td>
<td>Test environment</td>
</tr>
<tr>
<td>Platform</td>
<td>Security Policies</td>
<td>Change Management</td>
<td>HRM</td>
</tr>
<tr>
<td>Windows/Linux management</td>
<td>Information Risk Management (IRM)</td>
<td>IT Operations Schedule</td>
<td>Background Checks</td>
</tr>
<tr>
<td>Hosting</td>
<td></td>
<td>Event Management</td>
<td>Training</td>
</tr>
<tr>
<td>Network</td>
<td></td>
<td>Service Catalogue</td>
<td>Staff Agreements</td>
</tr>
<tr>
<td>Connectivity</td>
<td></td>
<td>Service Level Management</td>
<td>Contracts</td>
</tr>
<tr>
<td>Segmentation en firewalling</td>
<td></td>
<td>Capacity Management</td>
<td>Liability Management</td>
</tr>
<tr>
<td>Monitoring</td>
<td></td>
<td>Availability Management</td>
<td>Contract Management</td>
</tr>
<tr>
<td>Physical Infrastructure</td>
<td>Assurance</td>
<td>Release Management</td>
<td>Intellectual Property</td>
</tr>
<tr>
<td>Datacenter facilities</td>
<td></td>
<td>Asset Management</td>
<td></td>
</tr>
<tr>
<td>Housing</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Guidance for projects:

**Every service has a consumption label**

<table>
<thead>
<tr>
<th>Service Label</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Input</strong></td>
</tr>
<tr>
<td><strong>Output</strong></td>
</tr>
<tr>
<td><strong>Contact details</strong></td>
</tr>
</tbody>
</table>
Making it consumable
The SABSA lifecycle

SLA report
User feedback
Audit report
Service report

Manage & Measure

Strategy & Planning

Impl. at System A
Impl. at System B
Impl. at System C
Impl. at Systems A, B, C

Security Requirement R1

Actor: Service Manager
Actor: Auditor
Actor: User
Service attributes (1)

Core taxonomy:
• ID
• Name
• Short description (< 15 words)
• Parent service / related service

Security Service (Example)

<table>
<thead>
<tr>
<th>Architectural Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical</td>
<td>Validate the integrity of received messages by comparing them to a digital signature to detect if the contents have been altered during transit. Protect the integrity of sent messages by digitally signing them, enabling a recipient to validate that the contents have not been altered during transit.</td>
</tr>
</tbody>
</table>
| Physical            | • Digital Signatures  
                     | • Data Signing  
                     | • Hashing |
| Component           | • Approved Cryptographic Algorithms  
                     | • Approved Hashing Algorithms  
                     | • Approved Configuration  
                     | • Messaging Protocols  
                     | • Hardware Security Modules (HSM) |
| Service Management  | • Configuration Management  
                     | • Information Security Incident Response and Management |
Service attributes (2)

Design phase:

• How it works (in generic functional terms, no functional or technical design here)
• Input
• Output
• Business case for this service
  – What business goals are depending on this service
  – What business risk does it reduce
  – What compliance requirement is met by this service
• Risk type addressed by this service
  – Residual risk (likelihood, impact)
• How it helps in an in-depth-defence strategy (preventive, corrective, etc)
• How it helps in a multi-tier strategy (people, process, application, data, etc)
• Difficulty / required organization maturity level for this service
• Reference to control framework (ISO27002, SANS Top 20, COBIT, etc)
• Popularity rating (how popular is this service within the community)
Service attributes (3)

Implement phase:

• Ownership
• Contact details
• Features
  – Baseline features → suitable for what risk level?
  – Additional features
  – CIA rating (if classification scheme exists)
• Limitations to usage
• Interfaces (management, input, output)
• Costs to
  – Plan
  – Build
  – Deploy
  – Operate
• Total costs of ownership (1-3-5 year trend)

Manage and Measure phase:

• Metrics (security service level)
• Performance characteristics
• Maturity level
• Status (% deployed in environment)
<table>
<thead>
<tr>
<th>Service Group</th>
<th>Level 2 sub</th>
<th>Level 3 sub</th>
<th>Level 4 sub</th>
<th>Level 5 sub</th>
<th>TermID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SM1</td>
<td>Information Security Management is the corporate organization of information security which assigns ownership of security risks and defines the security management responsibilities and processes. Security management processes include risk assessment, the definition of control objectives, the definition and proper implementation of security measures, reporting about security status (measures defined, in place, and working) and the handling of security incidents.</td>
</tr>
<tr>
<td>Information Security Policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SM2</td>
<td>Information security policy is a set of policies issued by an organization to ensure that all information technology users within the domain of the organization or its networks comply with rules and guidelines related to the security of the information stored digitally at any point in the network or within the organization’s boundaries of authority.</td>
</tr>
<tr>
<td>Organization of Information Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SM3</td>
<td>.... Etc</td>
</tr>
<tr>
<td>Roles and Responsibilities assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SM4</td>
<td>.....</td>
</tr>
<tr>
<td>metrics and performance management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SM5</td>
<td>.....</td>
</tr>
</tbody>
</table>
TIMELINES
Initial planning

- Q2 2014
  - Finalize project charter
- Q3 2014
  - Set direction at SABSA World Conference, Naas, Republic of Ireland (September 2014)
    - Create a first version of the Security Services Catalogue.
      - We’ll use an approach that allows everyone to contribute. All contributions are welcome. There will be structuring of the material based on ‘group wisdom’, but not on consensus. This will result in a practical take-away for every participant.
- Q4 2014
  - Write Security Services Catalogue definition
  - Create or adopt Security Services Catalogue landscape
  - Present at The Open Group conference, London, October 20-21, 2014
- Q1 2015
  - Write SABSA practitioner guidance
- Q2 2015
  - Write TOGAF practitioner guidance
  - Present at The Open Group conference, Madrid, Spain, April 20-23, 2015
- Q3 2015
  - Create and publish first version of Security Services Catalogue
- Q4 2015
  - Set up maintenance process for the Security Services Catalogue
Short-term activities

• Gather information
  – Everyone: contribute to the service group that you know best
  – Group captain: collect the info in Excell tab, conform example

• Normalize the information
  – Group captain

• Create one taxonomy
  – (Co-)lead

• Vote for services
  – Everyone (👍)

• Publish final set
How can you contribute?

We appreciate your support

Please send an e-mail to p.de.koning@sabsa.org with:
1. The reason why you participate
2. The (3-5) service groups that match your expertise
3. An indication if you are open for the group captain role