Knowledge Solutions

**Security and Quality Management** -
The significance of the Information Security Management System (ISMS) and how to adopt it within your QMS.

March 2022
Quick Look: 3rd-Party Cyber-Risk Mitigation by Using ISO Standards

How Information Security and Business Continuity are Linked (w/ Willy Fabritius) - YouTube

Quick Look: 3rd-Party Cyber-Risk Mitigation by Using ISO Standards

Quick Look: 3rd-Party Cyber-Risk Mitigation by Using ISO Standards - YouTube

Willy Fabritius,
Global Head Strategy / Business Development

https://www.linkedin.com/in/fabritius/
SGS in Brief

No 1 World Leader
93K Employees
2 600 Offices
11 Global Industries

Our History

1878
SGS is founded

Mid 20th Century
Diversified into inspection, testing and verification services

1981
Listed on the Swiss Stock Exchange

Today
140+ years in business
Knowledge Solutions

Certification
Ensuring the quality and consumer safety of products and services.

Training
Improving employee competence and professional development.

Customized Audits
Assess and improve the performance of business operations.

SGS Transparency-One
Minimize supply chain risks by gaining visibility of your suppliers.

Technical Consulting
Improve productivity and operational efficiency.
The SGS Difference

Global and local experts, partnering with industry and regulatory associations

End to end partner

Number one global leader, with offices spread in over 80 countries

Industry Expertise

Quality of Service

Global Network
SGS Cyber Solutions

OUR SERVICES

- ISO 20000: IT Service management
- ISO 22301: Business continuity management systems
- ISO 27001: Information security management systems
- ISO 27017: Information security controls for cloud services
- ISO 27018: Protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO 27701: Privacy Information Management System
- WLA-SCS-2020: The standard for WLA members give assurance to all their stakeholders that security is one of their highest priorities
- GDPR Certification: delivers gap analysis and certification of compliance
- Penetrative Testing: provides a picture of cybersecurity resilience and the weak points in infrastructure and processes.
- Supply Chain Audits: a vendor audit program to independently assess compliance across the supply chain

<table>
<thead>
<tr>
<th>SERVICE OFFERING</th>
<th>CLOUD</th>
<th>INFORMATION SECURITY</th>
<th>DATA PRIVACY</th>
<th>AVAILABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 20000</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>ISO 22301</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>ISO 27001</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>ISO 27017</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>ISO 27018</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>ISO 27701</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>WLA-SCS-2020</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>GDPR Certification</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Penetrative Testing</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Supply Chain Audits</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
Introduction to ISO/IEC 27001

What is an ISMS
Benefits and purpose of ISO/IEC 27001

What are some of the worrying Trends in Information Security

As a quality manager I am worried more about supply chain availability, why should I worry about Information Security?

What is the connection between Quality and InfoSec
What is in it for me? Why should I, the quality manager / Director spearhead the InfoSec or BCMS initiative in my company?
How much effort does it take to add ISO/IEC 27001 to a current QMS implementation?
Information Security seems so technical

I am not an IT person. Do you need to be a cyber security expert to implement ISO27001?

And what kind of resources are needed to do so?
We have already our IT department taking care of this ---- why should I get
involved?

Will ISO27001 support our efforts at compliance with government regulations?
What about Client / OEM requirements?

Does every company need ISO27001, or is it for specific industries?
What other standards are there that fit to my specific use case or that I should
be aware of?

Does ISO27001 also make me compliant with data privacy regulations?
What does a typical 27001 certification process look like, if you are already 9001 certified? How long does it take?
Certification process

**Application & Quote**
Obtain a quote for your certification project

**Competence**
Identify any skill and competence gaps your staff may have

**Gap Assessment**
Identification of any weaknesses

**Stage 1**
Confirmation that the implementation of the management system is the right track.

**Stage 2**
Confirmation that the management system is fully implemented

**Certification**
Share your success with the world

**Ongoing improvement**
Regular surveillance visits will ensure your management system

**Ongoing improvement**
Regular surveillance visits will ensure your management system
How can SGS help me with learning more about ISO27001 / Information Security? Do you offer any trainings or courses on the subject?

How about certifications? Who do I talk to if I want to get certified?

There are many course providers and companies offering certifications out there, why should I go to SGS?
Thank you!

Do you have any questions?
Reach out to our team:
Willy.Fabritius@sgs.com

Visit our website, to learn more about our certification and training services