SC 27 Journal
Volume 3, Issue 2, July 2023

JTC 1/SC 27
Information security, cybersecurity and privacy protection
VOLUME 3, ISSUE 2

27001 BUSINESS EXPERIENCES CONFERENCE

5TH JULY 2023
The views and opinions expressed in the articles in this Journal are those of the author(s) and do not necessarily reflect the views or opinions of ISO, IEC, JTC 1, SC 27 or the editor of this publication.

ISO, IEC, SC 27, the editor and the authors shall not be liable regarding the use, interpretation or implementation of the material contained in any of the articles contained in this publication.

© ISO 2023
PROLOGUE

Welcome to Issue 2 (Volume 3) of the ISO/IEC JTC 1/SC 27 Journal. The purpose of Journal is to present articles from SC 27 experts involved in the development of standards covering information security, cybersecurity and privacy protection, and presentations from users of the SC 27 standards.

ISO/IEC 27001 has without doubt been a great global success story. In 2022, the third edition of the standard was published (https://www.iso.org/standard/82875.html). Of course 2022 was a bumper year for other supporting security standards - the third edition of ISO/IEC 27002 (https://www.iso.org/standard/75652.html) and forth edition of ISO/IEC 27005 (https://www.iso.org/standard/80585.html) were also published.

This current issue covers the conference that took place on the 5th July 2023, with the theme “27001 Business Experiences”. Presentations were provided by business professionals from eight different countries. These presentations provided valuable insight into how 27001 is being used in a variety of business scenarios. These reflect the importance and success of 27001 in the world of business. Thanks go to all speakers for their time and effort in developing and presenting their business experiences. Both the conference audience and SC 27 appreciate the speakers involvement in the conference.

Any questions or feedback relating to the content of this Journal can be directed to editor (sc27.wg1.edwardjh@gmail.com)

Dr Edward Humphreys
SC 27 Journal Editor
July 2023
INTERNATIONAL COMMON LANGUAGE

Dr Edward HUMPHREYS (SC 27/WG 1 Convenor)

COMMON LANGUAGE FOR RISK MANAGEMENT

ISO/IEC 27001 is the international common language for information security management. It is the lingua franca between organizations that may be involved in different types of sectorial business but they share a common goal - to manage and mitigate the information security risks all organizations are exposed to. ISO/IEC 27001 builds bridges and makes connections between organizations all communicating in the language of information security and associated risk management [1].

BENEFITS OF A COMMON LANGUAGE

Adopting an international common language for information security management provides many benefits - it is a trade language to facilitate trade and to connect economies, it is a language of best business practice, it is a language used by business managers, industrialists and technologists to exchange ideas on effective information security management solutions to mitigate risks [2], and it is a language to measure and demonstrate that an appropriate level of information security performance.

HISTORY

The historical development of establishing an international common language for information security and ISO/IEC 27001 is over thirty years in the making. Although the first edition of ISO/IEC 27001 was published in 2005, the standard existed as a national standard well before this and research into such a standard began in the late 80s. This historical development
brought together various initiatives, especially the movement and growth of security management away from the traditional ideas of IT security. This movement transformed security into a subject to be addressed by CEOs, boardrooms, business managers and away from the IT department. Like other forms of risk and business impacts, information security risk became a topic featuring on the agenda of management meetings and the subsequent impacts of information security risk became an important component of business decision making. [2]

CONFIDENCE, ASSURANCE AND TRUST

Building confidence, assurance and trust that cyber risks are being managed effectively is an important aspect of ISO/IEC 27001. This is an important goal of any and all ISO/IEC 27001 implementations and a goal that all organizations need to strive towards for the benefit of their stakeholders, the survivability of their business and their investments.

Conformity assessment helps build confidence, assurance and trust through a demonstration that a management system, product, person or service meets the specific requirements of a standard. Certification is one particular conformity assessment activity that provides this confidence, assurance and trust that a system, product or person meets the defined requirements. For example, written assurance (certificate) by an independent body an information security management system meets the requirements specified in ISO/IEC 27001.

CERTIFICATIONS

The first preliminary ISMS certification scheme was launched in 1997 and this was formalised in 1998, and the demonstration of conformance was against the requirements of the standard BS 7799-2 (forerunner of ISO/IEC 27001). Now, twenty-five years later ISMS certification has become an international way of doing
business, a means of providing confidence and assurance to all interested parties that your ISMS conforms to the requirements of ISO/IEC 27001. Such interested parties include business partners, customers and clients, shareholders and investors, and government regulators.

ISO/IEC 27001 is applicable to all types and size of business, covering all market sectors. It has become one of the very high profile and best selling standards from ISO. This success is also reflected in the number of ISMS certifications that have been carried out and has surpassed all expectations.

CERTIFICATION BODIES

The process of ISMS certification is undertaken by independent conformity assessment bodies (CABs). These CABs undergo a process of accreditation carried by a national accreditation body normally in the country the CAB is located. This accreditation process demonstrates the competence of the CAB to able to provide certification services that meets the requirements of an accreditation standard. In the case of ISO/IEC 27001, these accreditation standards are ISO/IEC 17021-1 and ISO/IEC 27006-1, respectively.

ACCREDITATION BODIES

The International Accreditation Forum (IAF) is the world association of Conformity Assessment Accreditation Bodies and other bodies interested in conformity assessment in the fields of management systems, products, services, and personnel. To find an accredited certification body, contact the national accreditation body in your country or visit the IAF pages https://www.iafcertsearch.org/search/certification-bodies.


[3] HUMPHREYS, Edward Dr - Is 27001 Just a Number? (to be published late 2023)
CONFERENCE PROGRAMME

KEY NOTE

International Common Language for Information Security Management
Dr. Edward HUMPHREYS

BUSINESS EXPERIENCES OF ISMS

ISMS Standard Practice and Thinking in Complex Context
Harry LIU (Huawei Technologies Company Ltd, China)

Experiences in the ISO/IEC 27001 Implementation Journey – A South African Context
Steve SIMMONDS (Wolfpack Information Risk (Pty) Ltd, South Africa)

Delivering trust and value in B2B services with 27001
Dr Ian Gregory (AdvanceTrack Outsourcing, UK)

27001 for ISMS in Mobile Networks
Francois ZAMORA (Orange Europe Division, France)

Metaforce - an SME’s ISO/IEC 27001 journey
Johan JUNGE - (Metaforce, Sweden)

Contributions of ISO/IEC 27001 to the evolution of the CyberSecurity ecosystem
Elder ARRUDA (Getnet, Brazil)

What value we see from the Implementation and certification of ISO/IEC 27001
Maribel Cisneros PEDREGUEIRA (CAAAREM, Mexico)

Protecting the Patient with a Secure Platform
Cory HILDEBRANDT and Faud KHAN (Auxita, Canada)
SPEAKER PRESENTATIONS
International Common Language for Information Security Management

Dr Edward HUMPHREYS
ISO/IEC JTC 1.SC 27/WG 1 Convenor
ISO/IEC 27001 – Digital World

ISO/IEC 27001 has opened up a world of opportunities and benefits for protecting the digital environment that supports business, government and society.

Its global outreach serves to protect organizations of all sizes, in all types of business and in the majority nations and regions of the world.
ISO/IEC 27001 – Common Language

• Most wide-spread of international standards for information security management
• It serves the global community with a means of communicating information security management across all types of business and all business sectors.
• All organizations irrespective of their sectorial business share a common goal – the means to manage and mitigate the information security risks all organizations are exposed to.
BS 7799-2
(Information security management system – Requirements)

ISO/IEC 27001
(Information security management system – Requirements)

WHAT’S NEXT?
FUTURE???
Panel Session
Discussion

1997 (1st edition)
2000 (2nd edition)
2005 (1st edition)
2013 (2nd edition)
2022 (3rd edition)

BS 7799-1 (1995)
BS 7799-2
ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27000, ISO/IEC 27001, ISC/IEC 27002,
ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005,
ISO/IEC 27006, ISO/IEC 27007, ISO/IEC 27008,
ISO/IEC 27010, ISO/IEC 27011, ISO/IEC 27013,
ISO/IEC 27014, ISO/IEC 27017, ISO/IEC 27019,
ISO/IEC 27021, ISO/IEC 27028 ... (40+ in the family)

(ISO/IEC 27000 Family of Standards and related standards)
ISO/IEC 27001 Certificates

The market take up of ISO/IEC 27001 ISMS certifications and registrations has been remarkable, with the number of certifications continually growing year by year since the dawn of ISMS assessments back in 1998.
ISO/IEC 27001 Sectors

- Aerospace
- Agriculture, farming and fisheries
- Automotive
- Biotechnology and life sciences
- Capital goods
- Communications
- Commercial and professional services
- Construction
- Consumer goods and products
- Education
- Energy
- Entertainment
- Finance and insurance
- Food industry
- Healthcare sector
- Logistics and supply chain
- Manufacturing
- Media and broadcasting
- Pharmaceuticals
- Retail
- Technology and software services
- Transport
- Utilities

% country take-up

- 7% (1999)
- 15% (2003)
- 30% (2007)
- 40% (2010)
- 78% (2019)
<table>
<thead>
<tr>
<th>Title</th>
<th>Speaker/Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experiences in the ISO/IEC 27001 Implementation Journey – A South African Context</td>
<td>Steve SIMMONDS (Wolfpack Information Risk (Pty) Ltd, South Africa)</td>
</tr>
<tr>
<td>27001 for ISMS in Mobile Networks</td>
<td>Francois ZAMCRA (Orange Europe Division, France)</td>
</tr>
<tr>
<td>Protecting the Patient with a Secure Platform</td>
<td>Cory HILDEBRANDT (Auxitz, Canada) and Faud KHAN (twelvedot, Canada)</td>
</tr>
<tr>
<td>ISMS Standard Practice and Thinking in Complex Context</td>
<td>Harry LIU (Huawei Technologies Company Ltd, China)</td>
</tr>
<tr>
<td>Metaforce - an SME’s ISO/IEC 27001 Journey</td>
<td>Johan JUNGE - (Metaforce, Sweden)</td>
</tr>
<tr>
<td>What value we see from the implementation and certification of ISO/IEC 27001</td>
<td>Maribel Cisneros PEDREGUERA (CAARREM, Mexico)</td>
</tr>
<tr>
<td>Delivering trust and value in B2B services with 27001</td>
<td>Dr Ian Gregory (AdvanceTrack Outsourcing, UK)</td>
</tr>
<tr>
<td>Contributions of ISO/IEC 27001 to the evolution of the CyberSecurity ecosystem</td>
<td>Elder ARRUDA (Getnet, Brazil)</td>
</tr>
</tbody>
</table>
Jan BRANZELL (Veriscan, Sweden)

Lars SUDLUND (Uppsec AB, Sweden)

The FUTURE for this Common Language

Pablo CORONA FRAGA (NYCE, MX)

PANEL SESSION
thanks for listening

Dr Edward Humphreys
Sc27.wg1.edwardjh@gmail.com

ISO/IEC JTC 1/SC 27
27001 Experiences Conference
5th July 2023
Experiences in the ISO/IEC 27001 Implementation Journey – A South African Context

https://www.wolfpackrisk.com
info@wolfpackrisk.com

Classification: Public
Version: 1.0
Cybersecurity Landscape in South Africa

According to INTERPOL South Africa is the cybercrime hub of Africa

In 2022, South Africa had 230 million threat detections in total. In second place was Morocco at 71 million.

Of the 230 million detected threats in the country, 219 million were e-mail-related threats. South Africa also had the highest targeted ransomware and business email compromise (BEC) attempts.

The exploitation of these cyber vulnerabilities within South Africa was further highlighted by Accenture, who identified that South Africa has the third highest number of cybercrime victims worldwide, at a cost of R2.2 billion a year.

The scale of cyber criminality in the country is further evidenced by the fact that the country saw a 100% increase in mobile banking application fraud and is estimated to suffer 577 malware attacks an hour.
So, What About ISO 27001?

ISO 27001 compliance is becoming a must have in the digital era in South Africa, but is still a tick-box exercise for some

- The cause of this view is because many companies are being bombarded with requests from existing clients, new clients and tender applications that they must have implemented ISO 27001 and/or be certified as well.

- This leads to us as at Wolfpack receiving queries for assistance from companies to help them to put ISO 27001 policies, processes and procedures as soon as possible.

- This can be seen as positive for us however, often businesses feel that having certifications is something they need to satisfy clients and stakeholders but see little intrinsic value in compliance for themselves, which in reality of course is no: the case.

- Importantly although ISO Certification is not a legal requirement, but compliance is becoming a necessity as the information security space becomes more and more regulated companies that ignore this could well get left behind.
Some Challenges with ISO Implementations I experience

- Culture of company's / resistance to change
- Understanding the guidelines
- Seeing the ISO 27001 implementation process as just too much work
- Lack of proper understanding of risk assessment and treatment thereof
- Scope of effort required (time and resources)
- Not understood that an ISMS involves everybody in the organisation
- Establishing and delegating responsibilities and ownership
- Getting Stakeholder (Top management) buy in
- Projects mostly delegated to IT Managers and not Information Security Managers
- HR and Legal Departments think the problem belongs to IT.
- Companies seeing ISO 27001 as a necessity for the wrong reasons due to pressure from potential and existing Clients and as well as tender application requirements
- The processes required get left behind in the frenzy to implement policies and procedures
Integrated Cybersecurity, Privacy and Resilience (CPR) Management Approach

Business Engagement


2. Establish Stakeholder Roles & Responsibilities

Risk Management & Execution

3. Assess Cyber Security, Privacy and Resilience (CPR) Controls

4. Implement a “Close the Gap” Strategy & Transformation Programme

Classification: Public
1. Risk & Opportunity Management Exercise (ROME)

Encouraging “Risk Based Thinking”

<table>
<thead>
<tr>
<th>LIKELIHOOD</th>
<th>IMPACT</th>
<th>Trivial</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very likely</td>
<td></td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>25</td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>20</td>
</tr>
<tr>
<td>Moderate</td>
<td></td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>15</td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>Rare</td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LIKELIHOOD</th>
<th>IMPACT</th>
<th>Critical</th>
<th>Major</th>
<th>Moderate</th>
<th>Minor</th>
<th>Trivial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very likely</td>
<td></td>
<td>25</td>
<td>20</td>
<td>15</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td>20</td>
<td>16</td>
<td>12</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>Moderate</td>
<td></td>
<td>15</td>
<td>12</td>
<td>9</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td>10</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Rare</td>
<td></td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Which scenarios present the greatest opportunity & risk scenarios to your organisation?

Classification: Public
2. Establish Stakeholder Roles & Responsibilities

ACCOUNTABLE – ISMS Steering Group Resp to Board / Exco

Risk Management, Compliance & Governance

RESPONSIBLE – Senior Management

The new “business as usual”

1st Line of Defence – The Organisation

Own & Manage Risks within their Function & Processes

2nd Line of Defence – Specialist Functions

Define Requirements

Financial Control

Security

Compliance

Quality

Information Technology

Resilience

3rd Line of Defence – Independent Review

Advise & Assist

Internal Audit

External Audit & Other Independent Reviews

Classification: Public
Allocate roles and responsibilities to the risk controls using an integrated Management RASCI that refers to the ISO 27002:2022 Controls.
3. Assess Cyber Security, Privacy and Resilience (CPR) Controls

- Identify risks
  - Vulnerabilities
  - Threats
  - Assets
  - Impacts
  - Incidents
- Evaluate risks
  - Strategy, policy
  - Risk appetite or tolerance
- Treat risks
  - Mitigate
  - Share
  - Accept
- Handle changes
  - External obligations
  - Advisories, standards etc.
4. Implement a “Close the Gap” Strategy & Transformation Programme

Safeguarding of personal information will be considered as required in the controls mapping process.

ISMS Framework
- Assign project responsibilities
- Information security policy applied to the existing system as an additional document
- Defined policy
- Consensus driven scope of the ISMS
- Adoption
- Information security policy
- ISMS Scope Document
- Risk assessment for the scope of the ISMS
- Iterative management response
- Risk action reporting
- Agreement
- Risk actions and risk treatment responsibilities
- Prepare Statement of applicability
- A statement listing policy, programs, and responsibility
- Control objectives relative to risk – ISO 27002 Controls, etc
- Map objectives to risk
- Control objectives relative to risk – ISO and Non-ISO
- Perform an assessment of the current state of the processes
- Align processes to the ISOC 27001 Standard

Ongoing program integrated with the overall compliance and audit program
- Implement controls
- Corrective action
- Prepare for and undergo pre-audit for certification
- Certificate awarded
- Passed

Stage 1 Certification Audit
- Stage 2 Certification Audit

Classification: Public
ISO 27001 ISMS Initiation and Establishment Flight Plan Example

Milestone Description
- SEP: Initiate ISMS project
- OCT: Define scope and current state
- Nov: Establish ISMS
- Dec: Policies and Risk Treatment
- Jan-Feb: Implement ISMS
- Mar-Apr: Communication plan
- May-Jun: Security Controls Implementation
- Jul-Aug: Incident Response
- Sep-Oct: ISMS Operations document
- Nov: ISMS Framework
- Dec: ISMS Scope & Policy Management

Key ISMS Deliverables
- Project plan
- As is Doc
- Process current state and ‘To Be’ state
- Determine ISMS Project Scope
- ISMS and Info Sec Policy
- Info Sec Risk Assessment Report
- Info Sec Risk Treatment Report
- Statement of Applicability
- Communications plan
- Training and awareness
- Security Controls Implementation
- Incident Response
- ISMS Operations document
- ISMS Framework
- ISMS Scope & Policy Management
- Information Risk Management
- Structure & Reporting
- Measurement of Controls
- Management Review of ISMS
- Info Sec org charter
- Info Sec Roles & Responsibilities
- Standards, procedures, process and controls design
- Operations document
- Metrics
- Audit Documentation
- Certification
- Closure

Remediation Streams
- IT Risk Governance, Architecture and service management
- Security Strategy
- Controls Implementation / Remediation
- Information Security Awareness & Training

Classification: Public
Steve is the Head of the Advisory business unit at Wolfpack and is an experienced Management Systems Consultant with over 25 years of experience in the governance, risk, and compliance industry. One of his main interests is the development of integrated management systems that encompass several management disciplines such as information security, privacy, and business continuity amongst others.

He is an IMS (Integrated Management Systems) Lead Auditor, Member BCI-JK Certified Business Continuity Practitioner, member of IOCSA, and IMCSA, and a Past President of the South African Society for Quality.

steve@wolfpackrisk.com

Building 1, Pendoring Office Park, 299 Pendoring Road, Northcliff, South Africa.

(+27) 11 794 7322
info@wolfpackrisk.com

www.wolfpackrisk.com
www.alertafrica.com
Contact Us
We look forward to partnering with you

Operating in:
South Africa - Gauteng, KwaZulu-Natal & Western Cape
Saudi Arabia - Riyadh

Head Office:
Building 1, Pendoring Office Park,
299 Pendoring Road, Northcliff,
South Africa.

info@wolfpackrisk.com
https://www.wolfpackrisk.com
(+27) 11 794 7322

Classification: Public
Delivering trust and value in B2B services with 27001
Dr Ian Gregory - Chief Technology Officer
• Sell to Accountants - UK/Australia/North America
• Provide accounts/tax/payroll etc.
• Proprietary systems
• Founded 2003
• Four offices
Our BSI Journey

- 2013 - ISO9001 - Quality Management
- 2013 - ISO27001 - Information Security Management
- 2019 - BS10012 - Personal Information Management
- 2020 - ISO22301 - Business Continuity
- 2021 - ISO27701 - Privacy Information Management
- 2022 - ISO27001:2022
ISO 27001 Provides:

- Assurance for Customers
- Allows Directors to Sleep
- Framework to maintain this as we grow
• Are we doing everything we can?
• How do we know?
• Business Management System
• Continuous improvement
• Build ISO27001 into operational systems and processes
ISO 27001 Provides

• Assurance for Customers
• Allows Directors to Sleep
• Framework to maintain this as we grow
Thank you
27001 for ISMS in Mobile Networks

Francois Zamora, CSO & CISO for Orange Europe division

ISO/IEC JTC 1/SC 27
27001 Experiences Conference
5th July 2023
Agenda

• Orange and the use of ISO/IEC 27001
• Strong points from certification auditors
• 27001 Experience
• Perspectives
• 8th world brand of networks and digital services
• 42.5 Billion euros of annual revenue
• 271 million customers
• 5000+ shops
• 900,000 resellers

26 countries

140,000 employees

Europe
Belgium / Spain / France / Luxembourg / Moldova / Poland / Romania / Slovakia

Middle-East and Africa
Botswana / Burkina Faso / Cameroon / Côte d'Ivoire / Egypt / Guinea / Guinea-Bissau / Jordan / Liberia / Madagascar / Mali / Morocco / Mauritius / Central African Republic / Democratic Republic of the Congo / Senegal / Sierra Leone / Tunisia
Target
Net zero carbon
by 2040

-12.1% reduction in CO2 emissions between 2015 and 2021

€60 million Endowment of the Orange Nature fund dedicated to projects related to reforestation and restoration of natural ecosystems

36.3% of electricity consumed already from renewable sources

20.4% collection rate of used mobile phone in Europe

6,000 solar telecom sites deployed
99% of the population covered in 4G in our 8 European countries and 17 countries in Africa and the Middle East.

5G already launched in 6 countries:
- Romania
- Poland
- Spain
- France
- Luxembourg
- Slovakia
27001 certifications in Orange: since 2006!

- **2006**: Orange Poland

- **2007**: Orange Business Major Service Center, Turkey, Egypt

- **2009**: Orange Slovakia

- **2010**: Orange Romania, Orange Moldova, Orange Business MSC in Mauritius

- **2012**: Orange Spain

- **2014**: Orange Poland Mobile + Fixed 27001 + 22301

- **2016**: Orange Spain 27001 + 22301, Orange Ivory Coast, Orange Mali

- **2023**: Orange Business: 11 certified Major Service Centers in 4 countries, Europe division: Spain, Poland, Slovakia, Romania, Moldova.

- **2024+**: Orange Belgium (target)
Strong points from certification auditors

- Since 2006, constant success of 100% surveillance and renewals
- Business-oriented ISMS
- In phase with the evolutions of ISO/IEC standards
- Use knowledge bases (27005, EBIOS, MITRE)
- Business-driven management of operational records and documents
- Evidence of ISMS delivering continuous progress
- Integrated certification with ISO 22301 BCMS
- Integrated certification with ISO 20000 and 9001
27001 Experience in Orange

- 2-year learning curve for every ISMS deployment
- Group-wide policies and guidelines generate time savings
- Confirming Orange brand value as a trusted digital services provider
- A standardized vocabulary worldwide effective in multi-cultural and multi-stakeholder environments
- Huge time savings RFPs and contracts with partners
- Huge time savings with B2B thanks to pre-formatted statements and records
- Situational awareness culture achieved by decision-making levels
- Learning culture from security incidents
- Improvements in Telco operations, in particular asset management, vulnerability management, proactive threat detection
Improvements in risk assessment from ISO/IEC 27005:2022

Credit: EGERIE software (www.egerie.eu)
Challenges with 5G

- Adressing how virtualization and automation can change telco security
  - Telco Cloud by Sylva
  - Edge computing, Open RAN
  - Knowledge bases from ENISA
  - EUCC, EUCS, EU5G
METAFORCE - AN SME'S
ISO/IEC 27001 JOURNEY

Johan Junge, CEO
ABOUT METAFORCE

- Founded in 2003
- Cloud-based Customer Communication Management (CCM) platform – Centerpoint™.
- Centerpoint enables our customers to develop, produce, distribute/notify, archive and sign of all types of written customer communication, from documents to digital dialogs – in one single platform.
- Customers across the Nordics within non-life insurance, life & pension, banking, member organizations and public sector.
- 48% market share in life & pension, 44% in non-life insurance in Sweden.
ORGANIZATION

GEOGRAPHICAL PRESENCE
- Headquarters in Stockholm, Sweden
- Office in Tønsberg, Norway
- Sales representative in Copenhagen, Denmark
- Strategic partnerships cross the Nordics

ORGANIZATION
- Privately owned with founders as principal owners
- 20 FTE (as of March 2023)
- Majority in development and professional services
WHY IMPLEMENT ISO/IEC 27001?

- Always prioritized security and best practices throughout the development and delivery of our products.
- The shift from on-premise to cloud in 2015 required a more organized and proactive approach to risk management.
- ISO/IEC 27001 and adding 27018 controls to the SoA, facilitate proactive risk identification and mitigation within a manageable framework, extending beyond development and delivery.
- Moreover, ISO/IEC 27001 would give us a competitive edge by enabling faster cloud migration, positioning us ahead in our industry.
  - Enhanced understanding of information security risks and continuous compliance with controls to meet our own and our customers' requirements.
  - Streamlined sales processes for smoother navigation.
  - Increased deal flow and scalable business growth.
THE ISO/IEC 27001 JOURNEY

- Required a partner with a comprehensive understanding of our current situation and future goals.
- Essential requirements before addressing additional enhancements. Focus was to establish a manageable ISMS that allowed us to:
  - Get certified (of course)
  - Gain thorough understanding of risks and proactively mitigate them.
  - Implement processes that involve all of management and from there the entire company
  - Strengthen collaboration with customers and partners to address information security requirements, including regulatory and customer-specific needs.
- The ISO/IES 27001 project in short:
  - Learn from scratch
  - Very close collaboration with our partner
  - Start to certificate – first plan 6 months, but took about 1 year (calendar time)
CERTIFICATION PROJECT PLAN – OVERVIEW OF STREAMS

A. Rules (Doc)
1. Create InfoSec rules docs to be published in “Office Handbook” including Info Sec Policy
2. Update “Rules” as needed from activities from Risk Assessments (risk tool)
3. “Awareness of “Rules”” All personnel meeting

B. Activities (Controls/ Risk treatment plan)
1. Carry out 5 “Process” risk assessments supported by risk tool. Determine activities to treat risks and link to controls
2. Carry out risk treatment activities. Support by experts as needed
3. Follow up on activities done. Update risks in risk tool. Report to management

C. ISMS Management process (Doc)
1. Create ISMS description - DRAFT
2. Make final adjustments (CISO)
3. Approve by CEO
4. First “TEST” Management review (3-Hours)
5. Internal Audit + Formal things (docs etc.)
6. REAL Management review (1 Hour)

D. Certification
1. Request tender from Certification Body
2. Plan certification audit
3. Certification audit

PROJECT PRINCIPLES
- Let the risk process drive what we do
- Business always comes first – stick to the order of planned activities and just adjust the timeline
KEY TAKE-AWAY: THIS IS JUST THE BEGINNING

- Today, we are the leading cloud-based CCM platform in the Nordics, with most of our customers in the cloud or about to migrate.
- The growing significance of understanding and proactively addressing information security risks is paramount to our business and our customers' success.
- Some key take-away points that we learned on this journey:
  - Set the right priorities from the start to ensure progress - focus on the "must haves" before the "nice to haves", this is an ongoing journey with no “finish”
  - Discover a trusted partner who understands your current and future needs, guiding you through this ever-evolving journey – it’s easy to get lost in the jungle of information security!
  - As your company expands, the significance of working with information security in a manageable and comprehensible way grows – more customers and employees demand a solid structure!
  - Yes, these endeavors can be time-consuming, but they are also one of our greatest strengths - enhancing our approach to information security directly boosts our bottom line!
Q&A
Contributions of ISO/IEC 27001 to the evolution of the CyberSecurity ecosystem

Elder Arruda – Senior Information Security Manager

PagoNxt | Getnet
AGENDA
INTRODUCTION

We are a financial services company that captures and processes financial transactions. Cyber Security is a big priority for us. The project to adopt ISO27001 started in 2013. In 2014 we obtained our first certification. Our main objective with the certification was to build a management system capable of consolidating an information security management system to evolve in the maturity of our cyber security ecosystem.
01 Board support
The engaged executive board was essential for us to be successful in the evolution of ISO27001 in our company

02 Cyber Risk Management
Continuous risk management work is an important input to our cyber security strategy

03 Awareness
Cyber Security Culture for all staff

04 Incident Management
Notification process and indicators for cyber security strategy

05 Vulnerability Management
Coverage for all assets
Thanks!

My Contact:
elder.arruda@getnet.com.br
AGENDA

1. Intro to Auxita
2. What we do
3. Our approach to 27K
4. Long term goals

PLEASE ASK QUESTIONS AT ANY TIME

Auxita Public
INTRO

• Faud Khan, EVP, Technology
• 25+ years of engineering experience in finance, telecom, defense, and cyber
• 5 patent grants, 10 patents pending
• Been working with Auxita since 2016
• Joined 2021 as a member of the executive team
• Joined SC 27 in 2002 (CA Mirror)
WHAT WE DO

- We are a **PSP (Patient Support Programs) Platform**
- We provide a platform for pharma’s to offer programs easily to HCPs (Health Care Providers) in Canada

**Benefits:**
- This significantly reduces the amount of forms that are required by both the physician and patient
- Patients are more willing to follow-up and get the necessary treatment
- We integrate with EMRs to allow specialist to provide treatment without faxing medical records
- Ensure that all new features are evaluated at all stages of the development lifecycle are risk mitigated

*Auxita Public*
OUR APPROACH TO 27K

• Started when we launched the company back in 2016
• Executive leadership and board knew it would be foundational to the future of the company
• Development and platform were key risk aspects
• Stakeholders: Patients, Physicians/Clinics, Pharma, Regulators
• Critical Assets: Platform (web application & database), Medical data
• Over time created policies and procedures, created audit processes, evaluated all technologies being implemented, and trained our staff
• All of these are ongoing as we pursue our certification

Auxita Public
CHALLENGES TO OUR IMPLEMENTATION

• We are a startup (our focus is growing revenues and signing pharma)
• We are all remote
• Many of our staff have never experienced a formal security program before
• Determine how we could automate parts of our system without impacting speed to market for our new features
• Dealing with requirements for certifications that have applicability to us i.e. SOC 2
LONG TERM GOALS

- Add more features to our platform for decision making for physicians
- Additional automation of these complex workflows
- Meet or exceed regulatory requirements for data protection
- Ensuring de-identification of both patient and meta data collected
- Obtaining certification Q1 2024
CLOSING REMARKS

- Security was a foundational part of our organization, even at the early stages
- We embedded ISMS aspects day one!
- As a start-up, you can start small and grow the implementation with the company
- Your SDLC is your “key” function for risk management for a software company
- Ensure staff at all levels understand the commitment to security and privacy
- Making sure all staff understand their role in protecting the organization
- Build trust with partners, patients, and physicians with shared risk model
Thank-you for your time today!

Faud Khan
faud.khan@auxita.com
PANEL - THE FUTURE JOURNEY OF 27001

Chair - Edward HUMPHREYS
Panel -
Jan BRANZELL (Veriscan, Sweden)
Lars SODERLUND (Uppsec Sweden)
Pablo CORONA FRAGA (NYCE Mexico)

[Chair Edward Humphreys] - The purpose of this Panel Sessions is to explore the views from three of JTC 1/SC 27 leading experts in the field ISO/IEC 27000 family of standards, of the future of these standards. The future will need to take account of the international digital transformation movement and the associated emerging technologies. The future will also need to take account the needs to organizations that are deploying more than one management system standard and wish to integrate these in an effective and optimal way. ISO/IEC 27001 has been the one and only ISMS for almost 20 years, many professionals want to continue this to be the case from the next 20-30 years.

[Jan Branzell] - We who are involved in the development of standards often call ISO/IEC 27001" ISMS" a management system. But that is not correct as I see it, it is a management system standard. It is a document that helps organizations to manage in this case information security in their way of running the organization's business, in its management system. This is one aspect that I think is important to consider for continue the success of ISO/IEC 27001 in the future as an organization do not want to many standards to take into consideration to support their business. To enable ISO/IEC 27001 to be the “ONE” management standard to use for information and cybersecurity is key for increased usage.
But to be that “ONE” management system standard, a second aspect should be considered and that is the rapid development within technology. We have IoT as one factor among others that will have a huge impact on the market and AI is now the current buzz word. An ISMS according to ISO /IEC 27001 must then cover new technologies and need for an organization to manage this by one management standard.

We should NOT get fragmented so we will have one ISMS standard, then a management system standard for IoT, one standard for AI, one for cloud etc.

Further, some talks about integrated management systems but I think that is mainly from an audit perspective as an organizations management system covers other aspects, then what ISO standards do, such as budget, personnel, market, finance etc. So, integration is not the way forward to keep ISO/IEC 27001 on the top as I see it. On the contrary I think this is a risk if this is the focus of developing the standard in the future and not what the use of the standards shall provide.

The real opportunity for ISO/IEC 27001 to continue its success in the future lies in if we as standards developers and national bodies around the world can develop the standard to be the ONE. By providing a systematic management approach and coverage of information security in the wide sense, we can keep ISO/IEC 27001 to be the trustworthy reference between organizations.

[Pablo Corona Fraga] - ISO/IEC 27001 will likely continue to evolve to address emerging trends and challenges in information security and cybersecurity

Its adoption by Small and Medium Enterprises (SMEs), in comparison to the view of a standard traditionally adopted by
larger organizations due to the complexity and cost supposedly involved. However, as information security becomes more critical for businesses of all sizes, we may see a trend where more SMEs seek this certification. Incorporation of Emerging Technologies, as the standard will continue to evolve addressing risks associated with emerging technologies like cloud computing, industrial control system, artificial intelligence, Internet of Things, and quantum computing.

To facilitate integrated management systems, the ISO/IEC 27001 may see further alignment and integration with other ISO standards such as ISO9001 (quality), ISO 22301 (Business Continuity Management), ISO 20000 (IT Service Management), or integrating disciplines such as privacy with ISO 27701. We may see more regulators around the world recognizing or requiring ISO/IEC 27001 certification, especially in sectors with high data sensitivity.

[Lars Soderlund] - I foresee a lot of new legislation that will either use ISO/IEC 27001 as a baseline for designing requirements or as base for new sets of controls regulated from legislation. There will also be an ongoing development that different governance and auditing frameworks try to present themselves as competitors or replacements for an ISMS. Users will need to understand the difference between legal compliance and conformity assessments under accreditation. Looking forward, there will also be a much bigger focus on product and software security. This will also introduce interfaces with ISMS.

Threats will continue to evolve over time, often connected with new type of technology such as AI and quantum computing. But also technologies like virtualization will be affected by new emerging threats.
In regards of international standards there will be a review conducted of the basic requirements in ISO/IEC 27001. We will most likely see management systems developed by IEC which will relate to information security. There is also a great need for working together with other JTC 1 committees on harmonizing terminology, which would be of great value for end/users.
SPEAKER BIOS

Dr Edward HUMPHREYS

Dr Edward Humphreys started working on ISO security standards in 1982, during this time he has managed several standards groups including the convenor of SC 27/WG 1, which he still leads, and directs the development and maintenance of the ISO/IEC 27000 family of standards. He also the managed the development of the UK ISMS standards BS 7799-1 and -2, the forerunners of ISO/IEC 27002 and ISO/IEC 27001, and the ISMS accreditation standard EA 7/03 9 (now ISO/QEC 27006). He was a senior assessor for several accreditation bodies including UKAS. He has over forty years business experience in information and IT security. He is a professor at several universities and is the author of seven books on information and cybersecurity.

He is a Liveryman of the London Worshipful Company of Information Technologists (WCIT). He is also the recipient of several awards for his work on the development of ISO/IEC 27000 family of standards including the UK Wolfe Barry Gold Medal, the 1906 IEC award, and several Lifetime Achievement Awards that credit him as the ‘father of ISO/IEC 27001 and the family of ISMS standards’.

Francois ZAMORA (Orange Europe Division)

As Chief Security Officer and CISO for the Europe division of Orange, Francois is in charge of a multi-country security work streams to integrate security in IT and Network (ITN) transformation. Such transformation consists in introducing cloud technologies and infrastructures to support the future
generations of telecommunications networks. To anticipate the effects on architecture design and on operations requirements coming from regulatory, standardization and certification, Francois is closely teaming with the entire ecosystem (European industry, standardisation bodies and institutional representatives).

Before joining Orange’s Technology and Global innovation, Francois was successively at Orange’s Group Security Department where he lead the global security management system for the Group, one of the Group’s pillars for security governance in its Europe, Africa and the Middle East operations, the B2B division and spent two years in the United States in developing remote sensing business for mobile networks engineering.

Francois is member of various France-based professional clubs promoting risk management best practice such as the EBIOS Club, the CESIN, the Club of Business Continuity. He sits at President-elect of the French National Standardization Body national commission mirroring the joint ISO/IEC Sub-Committee 27 for the standardization of Information Security, Data protection and Privacy. Francois also provides lectures at University of Limoges, Telcom ParisTech and others institutions in France.

**Dr Ian GREGORY** (AdvanceTrack Outsourcing, UK) Ian is the CTO of AdvanceTrack Outsourcing which provides accounting services to many large accounting practices across the world. His career spans over 30 years, and began in engineering and academia, before moving into industry, management consultancy and then IT. He has successfully led the implementation of standards including ISO27001 in the business.
Steve SIMMONDS (Wolfpack, South Africa)
Steve is the Head of the Advisory business unit at Wolfpack and is an experienced Management Systems Consultant with over 30 years of experience in the governance, risk, and compliance industry in South Africa. One of his main interests is the development of integrated management systems that encompass several management disciplines such as information security, privacy, and business continuity amongst others and has been involved in the implementation of ISO management systems up to certification at numerous companies throughout his career.

He is a qualified Management Systems Auditor, Member BCI–UK Certified Business Continuity Practitioner, member of IOCSA, and IMCSA, a past Director of the South African Quality Institute and Past President of the South African Society for Quality.

Elder Vinicius Telles DE ARRUDA (Getnet, Brazil)
Experienced executive in Cyber Security and IT Risk Management. ISO27001 Senior Lead Auditor and PCI Engagement Board Member (Brazil).

Johan JUNGE (Metaforce, Sweden)
Johan Junge is the CEO of Metaforce, a Nordic-loading Customer Communication Management (CCM) company based in Sweden that specializes in automating and digitizing mission-critical customer communications across various sectors, including insurance, banking, and public sector. With a career spanning the intersection of market communication and technology, Johan has consistently focused on empowering both small and large enterprises to fulfill their customers' communication needs in a personalized and relevant manner by leveraging data and cloud technologies.
Johan will impart insights on the significance of delivering highly secure SaaS solutions and adhering to essential standards like ISO/IEC 27001. He will shed light on how such commitments are not merely necessities but also provide a distinct competitive advantage for their business.

**Harry LIUHAIJUN** (Huawei, China)
Cyber security and privacy protection expert, CISSP, CIPM
Responsible for cyber security and privacy protection governance, risk and compliance management.

**Pablo CORONA FRAGA**
Candidate for a PhD in Sciences, specializing in Data Science, holding a Master's in Information Technology Management and a degree in Computer Systems Engineering. Currently, he is the Business Development Director at NYCE, and serves as a strategic advisor and counselor for various public and private organizations in the Information Technology industry, Financial sector, Service sector, Public Administration, among others. His expertise lies in creating, validating, developing, and maintaining strategies for digital transformation, cybersecurity, data science, artificial intelligence, information security, personal data protection, IT service management, governance, business continuity, and software development.

He has been an international editor of the ISO/IEC 27001 standards for information security management systems, 27003 on ISMS implementation, 27005 on risk management, and has participated in the development of other standards such as ISO/IEC 27002, 27701, 27017, 27018, 27004 among others. Furthermore, he has served as Vice-Convenor of the ISO working group developing the 27001 standard series globally and
coordinated the “Information Security, Cybersecurity and Privacy Protection” committee for ISO in Mexico.

His leadership roles include serving as the Vice President for Digital Health and former Vice President for Cybersecurity at the Internet Association MX (previously AMIPCI) and Vice President for Government, Risk, and Compliance at the Mexican Council for Information Security and Cybersecurity (Consejo SI).
In academia, he is a professor in the Master's program for Information Technology Governance at the Ibero-American University, teaching Good Information Security Practices and professor of the Master's program in Law and Information Technology at INFOTEC Research and Innovation Center for Information and Communication Technologies, where he teaches Forensic Computing.

He is the author of the book “Practical Guide for Risk Management in the Cybersecurity Era” and the compendium “Practicum Cybersecurity 2022”. He served as a member of the Technical Advisory Committee for the Preliminary Electoral Results Program (PREP) for the 2018, extraordinary 2019 and 2021 electoral process at the National Electoral Institute (INE). He is also an editor and writer of compliance initiatives for the Federal Law on the Protection of Personal Data in Possession of Individuals. He is a certified lead auditor in Information Security Management Systems, Service Management, IT Governance, Risk Management, and Business Continuity.

**Jan BRANZELL**

Jan Branzell is CEO at Veriscan Security in Sweden. He has an international marketing background from automotive and the pulp and paper industry before working within security. Since more than 20 years he has as an expert in management of cyber and information security supporting on how to successfully use the ISO 27000 series standards within organizations ranging
from 10-100 000 employees. Jan’s approach to security is that it should be a positive contributor to and for the business. He is a member of the standards development committee in “ISO/IEC JTC 1 SC 27 Information security, cyber security and privacy” since 2003 as a Swedish expert and editor of some standards such as ISO/IEC 27003. He is also part of the management within ISO/IEC JTC 1 WG13 on Trustworthiness.

Lars SODERLUND