HOW TO SELL DIGITAL TRUST TO THE BOARD

Alexandra D'Archambeau
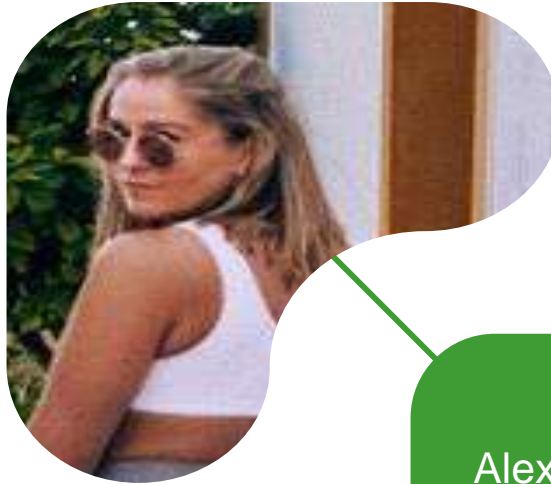
30 maart 2023

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

CONTENT

1. Who am I?

2. What is digital trust?

3. How to sell digital trust to the board?

4. Who do you want to hire and how to retain them?

HOW I WOULD DESCRIBE MYSELF **ISACA** STYLE

Most likely known from social media

Main holidays are usually in Portugal

Alexandra D'Archambeau

Primarily to be found on the golf course

Best local politician ☺

Alexandra D'Archambeau
Open VLD

I'm also a GRC professional with almost 6 years experience in ISO27k, privacy and security risk management.
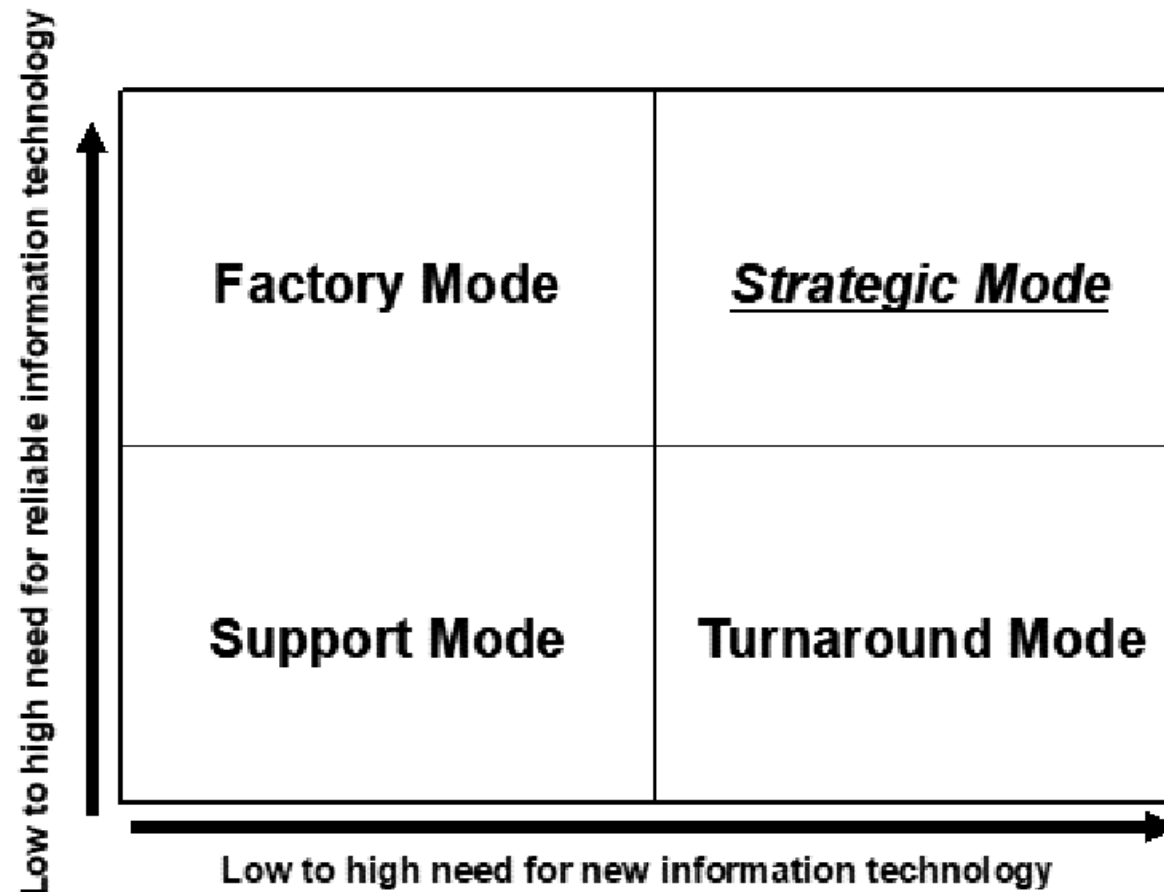
WHAT IS DIGITAL TRUST?

ISACA defines digital trust as the confidence in the integrity of the relationships, interactions and transactions among suppliers/providers and customers/consumers within an associated digital ecosystem.
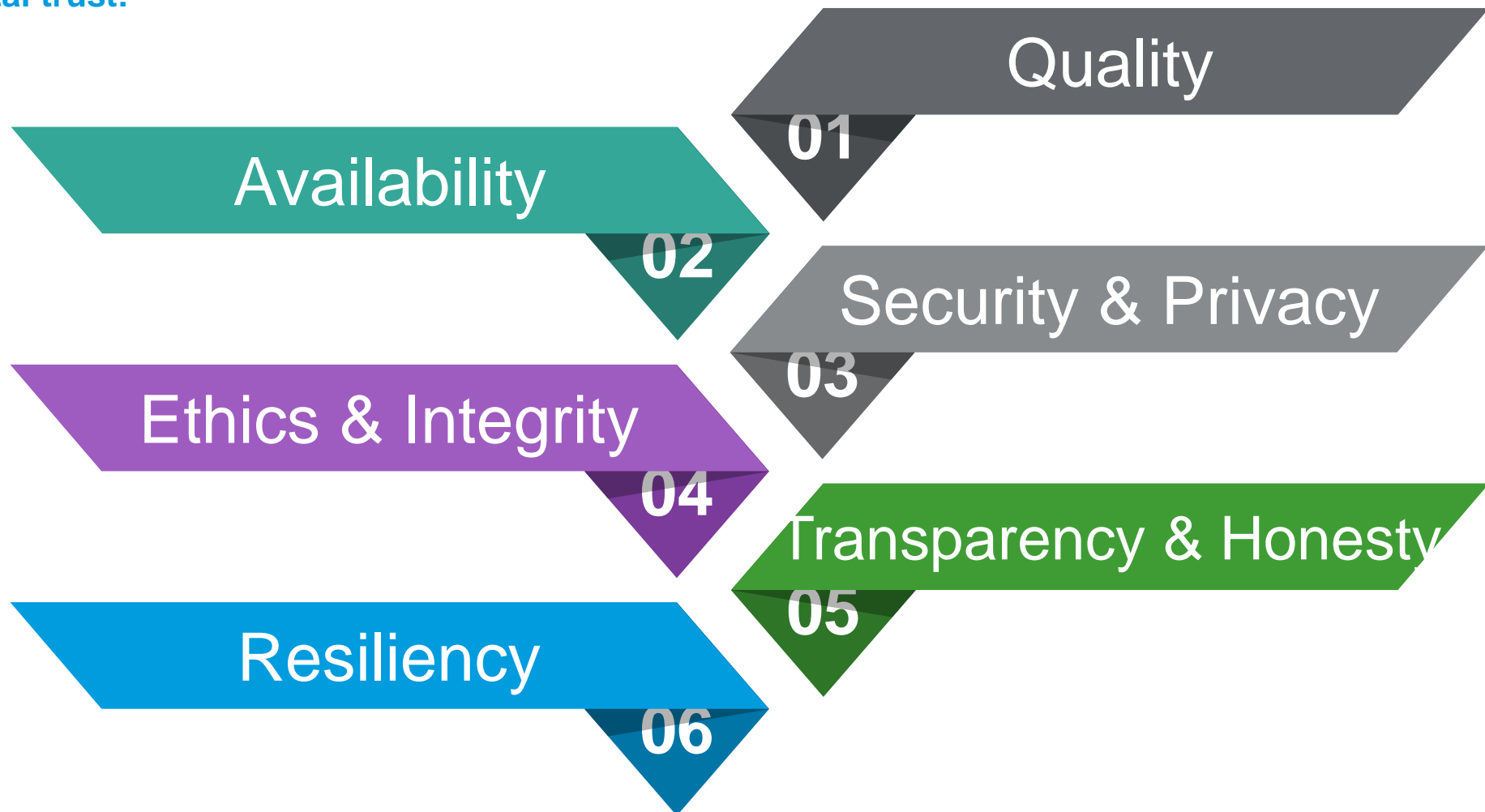
RSM

WHAT IS DIGITAL TRUST?

Digital transformation

WHAT IS DIGITAL TRUST? – CONSUMER PERSPECTIVE

Many customers' decisions are based on trust. ISACA mentions that customer's consider six factors when determining digital trust:

01 Quality

02 Availability

03 Security & Privacy

04 Ethics & Integrity

05 Transparency & Honesty

06 Resiliency

WHAT IS DIGITAL TRUST? – PROVIDER'S PERSPECTIVE

An enterprise needs assurance from its providers in order to provide trustworthy services to its customers.

HOW TO SELL DIGITAL TRUST TO THE BOARD?

RSM

HOW TO SELL DIGITAL TRUST TO THE BOARD?

City of Antwerp hit by cyber attack

Tuesday, 6 December 2022

Antwerp City Hall in the city centre, Thursday 22 October 2020. Credit: Belga /

HOW TO SELL DIGITAL TRUST TO THE BOARD?

Common issues:

1. CISO does not report to C-functions like CEO, CRO or CIO. Too low in the hierarchy of the organisation.

2. No or limited knowledge of IT and security amongst the BoD/Exec

    *   Underlying issue is lack of resources

The board doesn't understand cyber security nuances

"How much does the board/executive management understand cyber security implications?"

— None 27.9%   — Some 42.8%   — Quite a bit 19.9%   — A great deal 9.5%

| 27.9% | 42.8% | 19.9% | 9.5% |

Source: Getting Board Buy-in on Cybersecurity – Bulletproof.co.uk

"What would affect your bonus most?"

WHO DO YOU WANT TO HIRE AND HOW TO RETAIN THEM?

RSM

WHO DO YOU NEED TO HIRE?

WHO DO YOU NEED TO HIRE?

WHO TO HIRE

Key skill(s)	• Assess and enhance an organisation's cybersecurity posture • Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks • Analyse and comply with cybersecurity-related laws, regulations and legislations • Implement cybersecurity recommendations and best practices • Manage cybersecurity resources • Develop, champion and lead the execution of a cybersecurity strategy • Influence an organisation's cybersecurity culture • Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing • Review and enhance security documents, reports, SLAs and ensure the security objectives • Identify and solve cybersecurity-related issues • Establish a cybersecurity plan • Communicate, coordinate and cooperate with internal and external stakeholders • Anticipate required changes to the organisation's information security strategy and formulate new plans

Source: ENISA EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

WHO TO HIRE?

ChatGPT:

Key Soft Skills for a CISO

1. Communication Skills

- Able to communicate complex technical issues in simple terms
- Provide recommendations in a clear and concise manner

2. Leadership

- Ability to motivate and inspire their team
- Build a culture of security awareness

3. Adaptability

- Able to pivot quickly to address new security risks or threats
- Work under pressure and prioritize work in a fast-paced environment

4. Strategic Thinking

- Align security goals with broader business objectives
- Balance security risks with business needs

5. Collaboration

- Work collaboratively with other departments in the organization
- Build relationships with stakeholders and work towards a common goal

HOW TO HIRE

Job Description

Role:
Act as interim Chief Information Security Officer and/or GRC role for an organisation with tasks including:
• Agree cyber security ambition level with Board
• Make, agree and secure budget for security roadmap to achieve the agreed ambition level
• Manage, develop security organisation
• Manage security processes and tooling including purchase of new tools, licensing and security services
• Report on security status and maturity level to the Board and other stakeholders
• Manage security aspects of relationships with suppliers and customers
• Enforce regulatory requirements (e.g. GDPR)
Governance, risk and controls consultant with expertise areas in multiple areas such as:
• ISO 27000/1 or NIST framework implementation or certification preparation
• Design, set-up and embedding of security related processes (risk assessment, compliance, incident, awareness, governance, etc.)
• Operation of security related processes
• Reviews, audits of security related processes
• Set-up IT risk management and associated processes

HOW TO HIRE AND RETAIN THEM

BE CREATIVE

1. Employees will not come for your good coffee or great company culture, they will come for **flexibility** and a healthy work/life balance. Be remote-friendly!

2. **Think outside the box**: is a four-day workweek possible? Asynchronous work?

3. Employees will stay if there is good **talent management**.

4. **Coach** your managers! It's not because you/someone are/is a great CISO that therefore you/he are/is a born people manager.

5. Employees will come if you have a transparent and adapted **wage** policy. Companies are losing the battle against consultants!

This is not only a HR problem, this is also your problem.

Q&A