IT Security Services

Arco & Gäste
"Das Cybergespräch" LIVE

IT Security from a Software Sourcing Perspective is Vulnerability Avoidance

03. February 2021

Bertil Strub

Swiss Sourcing Group, President

SoftwareONE AG, Senior Consultant

bertil.strub@bluewin.ch

Bertram Dunskus *CISSP, M.Sc.*

CEO

Arco IT GmbH
Albulastrasse 34
8048 Zürich

+41 79 616 07 25

bdunskus@arco-it.ch

IT SECURITY SERVICES

Bertil Strub

SLM Senior Consultant

Activities Overview

- Head of Global Software Sourcing @ UBS
- Joined SoftwareONE in 2016
- Responsible for purchases of a large Bank
- SLM Senior Consultant for multiple customers in task force mode
- SLM Presales and analytics

Focus Areas and Specific Knowledge

- Project Management (PMI, Scrum)
- Negotiations with multiple large Software Publishers such as Adobe, IBM, Informatica, Microsoft, Oracle, Red Hat, SAP, Eri Bancaire, Temenos, SimCorp and many more
- Cost reduction experience by consolidation of product sets and focus on co-terminus renewals, reduction of volumes
- Spin-offs and contractual impacts to both entities

Professional Experience

- Cobol, Assembler, MVS on IBM Mainframe 10 Years Global Software Sourcing 20 Years
- Data Center Sourcing 2 Years
- Contract analysis and negotiation for M&A and Divestures 4 Years
- President of Swiss Sourcing Group since 5 Years

Diplomas / Certificates

- Swiss Banking Diploma
- CFA Program Curriculum for Banking
- Sourcing Batchelor University St. Gallen

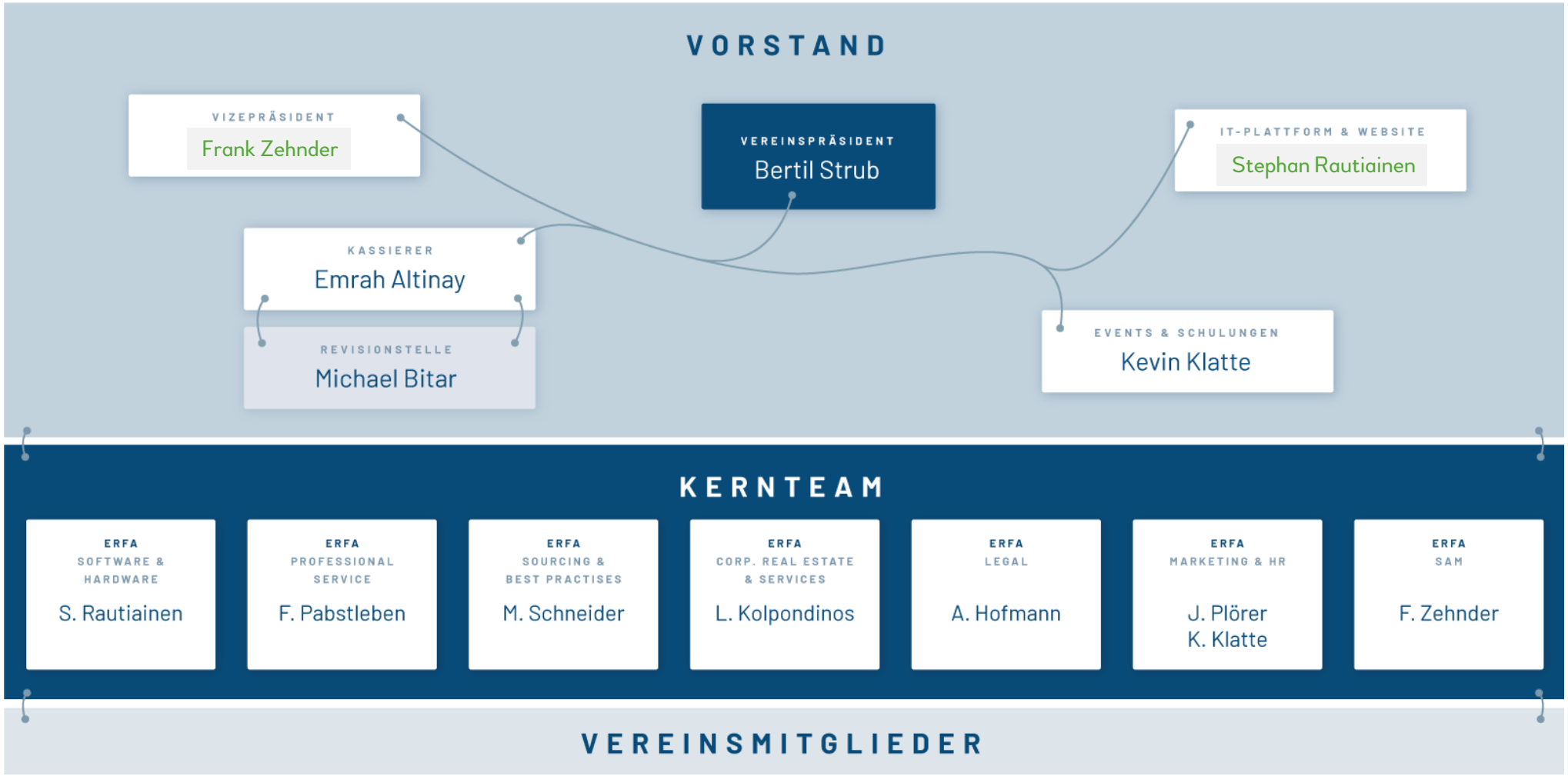
arco

IT Security Services

IT Security from a Software Sourcing Perspective

is Vulnerability Avoidance

Wer ist SSG ?


VORSTAND
VIZEPRÄSIDENT
Frank Zehnder
VEREINSPRÄSIDENT
Bertil Strub
IT-PLATTFORM & WEBSITE
Stephan Rautiainen
KASSIERER
Emrah Altinay
REVISIONSTELLE
Michael Bitar
EVENTS & SCHULUNGEN
Kevin Klatte
KERNTEAM
ERFA SOFTWARE & HARDWARE
S. Rautiainen
ERFA PROFESSIONAL SERVICE
F. Pabstleben
ERFA SOURCING & BEST PRACTISES
M. Schneider
ERFA CORP. REAL ESTATE & SERVICES
L. Kolpondinos
ERFA LEGAL
A. Hofmann
ERFA MARKETING & HR
J. Plörer
K. Klatte
ERFA SAM
F. Zehnder
VEREINSMITGLIEDER

Optimization opportunities
Facts from the market

Only **60%** of spend is “under management” by Procurement.

Source: CPO Agenda

30% cost reductions by enterprises that implement software asset management.

Source: Gartner, Using IT Asset Management to ensure Software Compliance

For **89%** of organizations surveyed the main SAM - Software Asset Management - initiative goal is compliance.

Source: SAMS Europe & USA Survey Report

35% actual measured amount of wasted public cloud resources reached

Source: Right Scale, State of the Cloud Report

66% of organizations are not satisfied with their current SAM and ITAM implementation.

Source: SAMS Europe & USA Survey Report

The Sales Person

The Customer View

WOW, this looks so great.

We must have this.

Sales Marketing

What you need, and what publisher might get

- If you store your data in their environment, read their rights on access and use
- Have your contractual statement ready to cover your data by encryption, confidentiality and audit clauses
- Ensure you have a data back-up outside of this environment
- In the case of a subscription/SaaS agreement, negotiate not to exceed terms for the subsequent year(s)
- Start negotiations early. The closer to the end of the term, the less time to consider switching and the greater the pressure to accept publisher conditions

What the Salesperson will get once you sign

What you need to read and negotiate

- Never ever allow employees to accept cloud click-through agreements

- These days it is all about unit pricing instead of TCO
  - Total Cost of Ownership
- There are so many other elements to be seriously considered

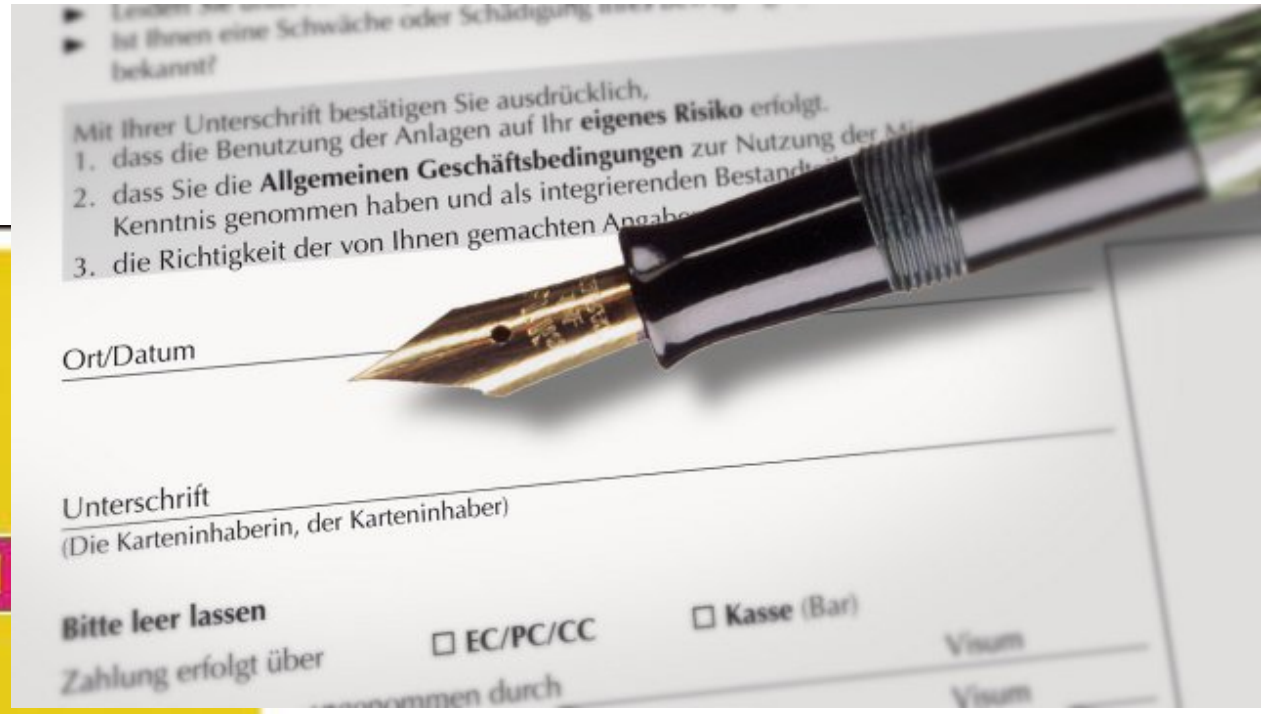
Is everybody aligned with what happens after signature?

Never buy
"a cat in a bag"

- Who has an impact on the purchase decision?
  - Business looking for solution (was it based on RfP?) / What will be replaced?
  - IT Security to test on malware; company standards/policies and data encryption
  - Compliance (Software to measure usage according to contract (SNOW, Flexera, ServiceNOW, etc.)) Is Blockchain involved in data transfer?
  - Legal contract review and change requests (EULA check)
  - Head of Sourcing
  - Budget holder (Business or IT if Infrastructure) Controller / Finance
- Do we have a testing period without purchasing obligations? Was this successful?
- Has penetration testing been successfully performed?
- Is Data Protection solid?
  - In the solution?
  - Access and password handling?
  - And in the infrastructure which will be used (on premises, in the cloud (private/public)?
  - Are all company mandatory policy and regulator obligations covered?

Seek Everybody's Agreement

Commitment



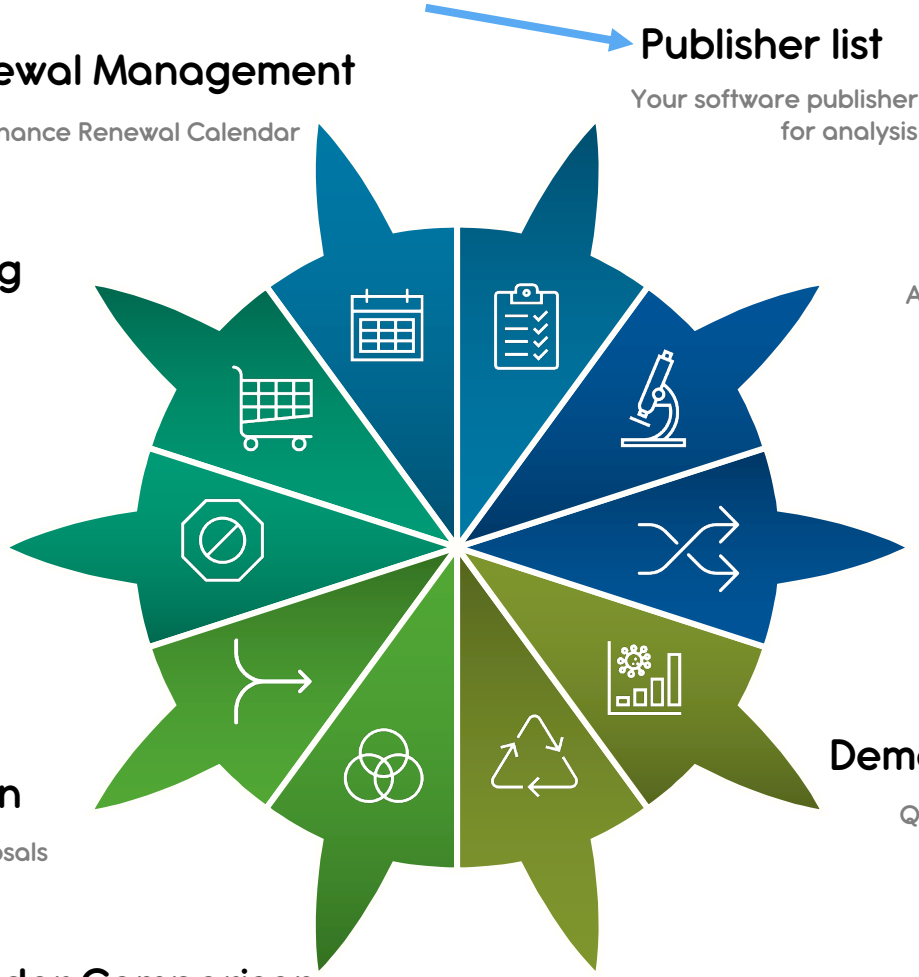
....the documents get stored and ignored while the operational IT world is changing

Hardware goes to museum – Software is running every night

As long as licenses are operationally active, they need to be under control by a SAM team to be audit ready at any time

- Up to 20% of purchased licenses are unused while company is paying maintenance or subscription fees
  → Cost optimization opportunity
- Up to 15% of installed licenses are not maintained
  → These licenses are most vulnerable to cyber attacks
- Up to 5% of installed licenses are running on extended maintenance support
  due to lack of timely upgrade implementation, or have switched to new solution
- Many comparable solutions are active due to:
  - Maverick purchases over time
  - Different approvers in individual divisions
  - Missing CTO and CISO enforcement
  - Missing budget to consolidate and standardize solutions
  - I have seen more than 15 different BI-Tools installed in parallel

Software Lifecycle Management



Publisher list

Your software publisher list as bases for analysis

Analysis of existing spend

Analyze list and classify vendor respectively (e.g. SW / HW / Consultancy vendor)

Correct Allocation

Change allocation for non-SW vendors

Demand Qualification

Qualify the demand

Assessment

Use, lose or reuse

Vendor Comparison

Compare functionality provided by publishers

Consolidation

Consolidation of proposals

Termination

Termination of discontinued solutions / contracts

Transaction Reselling

Order new period

Renewal Management

Maintenance Renewal Calendar

Purchase Optimization

Differences between Software Agreements, other purchases

- Except in greenfield scenarios, you need to transfer your data before you can retire the existing solution(s). This will cause license cost in parallel, plus migration cost
- Except perpetual licenses you only subscribe to a license right which will end at the term
- Perpetual licenses may only be upgraded as long as maintenance is paid for, or to the last available release level before maintenance expired
- All subscribed licenses may only be used during the subscription period. This is the case whether licenses are installed on premise or in the cloud. Mainly American companies like this license form due to cost allocation without any depreciation over time. This method however implies multiple vulnerabilities to the customer:
  - Licenses may not be used after license term
  - Licensor may increase prices at any renewal date substantially. You will not have time to migrate away in due time
  - Your data may not be accessible by an alternate solution or is stored in a format which will not fit to the new solution.
    You may have legal obligations to store data and make it available (gesetzliche Offenlegungspflicht)
    and to delete them according GDPR
  - Your data may be hosted in the cloud of the Licensor. Are you aware of their rights over your data?
  - Do you have a plan on how to back-up your data, or do you rely fully on the solution provider?

What can change after the documents have been signed?

- License quantities are changing (Use or Lose / True-up → to remain compliant)
- Additional modules available under same license key, but not contracted
- Hardware got replaced → licenses valid e.i. for 4 cores: hardware having now more cores available and entire server needs to be licensed (e.g.: Oracle)
- Hardware is providing more capacity; however, software is limited for a defined number of transactions
- Software is limited to geographical area
- Software is limited to named users
- T's & C's are changing with maintenance renewal or subscription extension → nobody took notice
- Political decisions/restrictions to use the software or to produce for specific countries/companies

Is the application owner aware of the contractual T's & C's and potential impact how to use licenses in the daily business?

Do you have a SAM Team managing usage over time?

Where do I store my data?

The question here is not about the storage media. It is all about how to conserve my data.

- ✓ Data is stored according the record definition within the respective application
- ✓ Consequently, I can read and process my data only as long as I can use the application
- ✓ Do I store the data in a format which will be accessible without the application?
- ✓ If solution is in the cloud, do I have an on-premise back-up?
- ✓ What is the impact in case my cloud provider is going out of business?

  (The biggest assets are not the hardware and the network, it is my data.)

  Do I have an Escrow agreement for the licenses?

The Customer View

- Do your homework continuously over time and be ready at any time to be audited
- Remember, the responsibility starts when signing the documents, maybe not in your business unit, but it is still the company's responsibility to remain compliant
- Responsibility will end after complete deinstallation
- Establish a renewal calendar allowing decisions to be taken prior the cancellation period

Q & A

Contact: bertil.strub@bluewin.ch

Bertram Dunskus *CISSP, M.Sc.*

CEO

Arco IT GmbH
Albulastrasse 34
8048 Zürich

+41 79 616 07 25

bdunskus@arco-it.ch

IT SECURITY SERVICES

Arco & Gäste "Das Cybergespräch" LIVE in 2021

- Swiss Cyber-Safe: Certification for SMBs
- Securnite GmbH: IT Security Assessments
- Basler Versicherungen: Cyber Insurance

... SUBSCRIBE to Arco IT Security Services channel

Arco & Gäste
"Das Cybergespräch" LIVE

IT Security from a Software Sourcing Perspective is Vulnerability Avoidance

03. February 2021

Bertil Strub

Swiss Sourcing Group, President

SoftwareONE AG, Senior Consultant

bertil.strub@bluewin.ch

IT Security Services