

# CCSP:RND

## Cloud Cyber Security and Privacy: Readiness for the Next Decade

---




Magnus Westerlund, Bob Duncan, Andreas Aßmuth, and Sebastian Fischer

Cloud Computing 2021 – Porto, Portugal






April 18, 2021 to April 22, 2021




## Dr. Magnus Westerlund

 Arcada University of Applied Sciences  
 Finland  
 [magnus.westerlund@arcada.fi](mailto:magnus.westerlund@arcada.fi)




## Dr. Bob Duncan

 University of Aberdeen  
 Scotland, UK  
 [bobduncan@abdn.ac.uk](mailto:bobduncan@abdn.ac.uk)

## Prof. Dr. Andreas Aßmuth

 OTH Amberg-Weiden  
 Germany  
 [a.assmuth@oth-aw.de](mailto:a.assmuth@oth-aw.de)

## Sebastian Fischer, PhD Candidate

 OTH Regensburg  
 Germany  
 [sebastian.fischer@othr.de](mailto:sebastian.fischer@othr.de)

During the course of the past decade cloud computing has resulted in an almost complete transformation of the IT landscape. The initial reluctance shown by many potential users to utilise public cloud infrastructure due to concerns about security and privacy has given way to greater acceptance following the ability to perform horizontal scaling securely and, in particular, for an economic cost, as compared with self-hosted dedicated hardware. As new software is created, it increasingly is designed as cloud-native solutions that can reap the benefits of the cloud. Monolithic designs are giving way to microservices, serverless, and unikernel designs, whose aim is to improve security, scaling, and cost effectiveness further. The COVID-19 pandemic also forced many people of all ages to use cloud services for video conferences, home schooling, etc., which has led to a significant increase in the number of users of cloud services.

Looking towards the coming decade, the transformation will likely not stop there and the new paradigm is already forming. As the capabilities of cloud continue to evolve and grow, rather more worryingly, so too do the capabilities of attackers. As was already seen in 2020, the increased usage caused by the pandemic made cloud services even more attractive as targets for cyber-attacks. Since new legislation and regulation is continuously being introduced, and some, such as GDPR, have exceptionally high compliance requirements coupled with a high level of punitive fines, it is necessary for companies who use cloud to take a much more serious approach to achieving compliance.

Failure to take appropriate measures to safeguard data held in the cloud will no longer be tolerated by regulators. Equally, failure to report breaches properly and timeously are also starting to be heavily punished by regulatory authorities. Looking at the current level of regulatory fines, it is clear that regulators are getting serious about enforcing better compliance. It is no longer possible for companies to sit back as see what everyone else does, now companies have to demonstrate a proactive approach if there is to be any prospect of a large reduction in the fines levied due to their efforts providing mitigation.

- Introduction  
*Chairs*
- IT Security of Cloud Services and IoT Devices in Healthcare  
*Michael Gleißner, Johannes Dotzler, Juliana Hartig, Andreas Aßmuth, Clemens Bulitta, and Steffen Hamm*
- An Approach for Decentralized Authentication in Networks of UAVs  
*Nicholas Jäger and Andreas Aßmuth*
- How to prevent misuse of loTAG?  
*Bernhard Weber, Lukas Hinterberger, Sebastian Fischer and Rudolf Hackenberg*

- A Secure and Privacy-Friendly Logging Scheme  
*Andreas Aßmuth, Robert Duncan, Simon Liebl, and Matthias Söllner*
- Incorporating Permanent Audit Trails for Corporates  
*Robert Duncan, Magnus Westerlund, and John Wickström*
- Open Discussion and Closing Remarks  
*Chairs (Moderators)*