Cloud Adoption
The COVID-19 crisis as the biggest accelerator for Cloud Computing?
1. **Situation and risks**
   a. COVID-19 crisis and the Cloud
   b. Clients in “COVID-19 mode” in “rush transformation”
   c. One step back to see the full picture

2. **Key topics – what our experts are saying**
   a. Make the cloud transformation sustainable
   b. Skill up, Clean up
   c. Compliance and data protection
   d. Opportunities of change emerging from the crisis

3. **Q&A – ask your experts now**

4. **Summary & key take-aways**
In the context of the COVID-19, Cloud solutions brought immediate benefits:

- Instant availability
- Rapid proof-of-concept
- Quick installation and configuration
- Ease of use
- Scalability
- Apparent cost-effectiveness (e.g., limited upfront investment)

However, in the long term, unconsidered cloud adoption presents risks that need to be assessed and mitigated to an acceptable level:

- Uncontrolled use of unapproved services ("shadow IT")
- Security challenges (e.g., data leakages, unauthorized access, dependence on a service provider to ensure adequate internal controls, extreme reliance on secure connectivity to the cloud)
- Privacy and regulatory compliance shortcomings
- Lesser control over availability and quality of service
- Underestimate of the “real cost” of moving to the cloud (e.g., runaway costs from poor planning)
COVID-19 crisis and the Cloud

Client view (examples from our clients)

Capacity Management
Customers where enabled to work from home, but because of inadequate capacity planning (VPN, Internet Access, VDI) part of the company had to work in the morning and part in the afternoon. Mobile devices were purchased and deployed in a rush.

Network Bandwidth and Design
Most of the employees where forced to work from home, but the network was not designed to split traffic and all the traffic went trough the central infrastructure, resulting in a network overload.

Identity Management
Microsoft Teams was implemented in a rapid approach to enable workers to collaborate. Identities where not synchronized the cloud solution, this results in users having multiple identities or need to login multiple times.

License Management
Customers took advantage of the free licensing offers by the several vendors. No proper long-term cost evaluation was considered (or budgeted)

Rapid adoption of modern workplace
Modern workplace enable the productivity on any devices. Policies, integration and operational procedures left behind in combination with a lack of monitoring capabilities increased the risk of successful attacks and a security operation not being able to detect it.

Data Protection Impact Analysis
We have seen that customers where willing to take more risks and short-cut also on data protection checklists before implementing technologies, this can result in putting data at risk or violating compliance or law.

Attacker view

Spike of phishing attacks
Criminals are creating fake sites related to COVID-19 to entice victims into opening malicious attachments. Trend Micro reported that nearly one million spam messages have linked to COVID-19 since January 2020

Vulnerabilities of working from home
Threat actors exploiting vulnerabilities of systems, networks and applications implemented as result of the rapid adoption. They are searching for exposure to steal data and make profit or cause disruption.
One step back to see the full picture – Samples of a cloud journey

- Business-, technology- and sourcing strategy aligned
- Business drivers and economic analysis
- Cloud business case, -strategy and -roadmap
- Vendor evaluation and 3rd party management
- Governance and policy management
- Risk, compliance and policy management
- Platform definitions
- Operations process definitions
- Hybrid identity and access management
- Cultural change
- Awareness, training, education, certification
- Roles, responsibilities, competencies
- Infrastructure & application inventory, profiling and strategy
- Cloud target state design, architecture design
- Dependency mappings
- Package and release Management
- Detection and response in hybrid environments
- Regulatory requirements collection and definition
- Privacy target state design
- Cloud privacy controls
- Cloud regulatory reporting
Now is the time to take a step back and review your rapid adoption.

For a successful cloud adoption we see the following key prerequisites:

- **Knowing Why**
  - COVID-19 as trigger

- **Having a Plan**
  - Rethink your approach
    - Review:
      - Strategy
      - Security
      - Operating Model
      - Organizational Change

- **Executive Sponsorship**
  - Cloud transformation impacts your business and drives business results
  - Executive sponsorship essential for successful implementation

- **Legal & Compliance**
  - Common understanding on:
    - Opportunities
    - Laws
    - Regulations
    - Restrictions
Key priorities to consider

What you can do

Review your approach – review your adoption approach using those key priorities:

1. **Upskilling** – Upskill your workforce in remote working and new working styles

2. **Develop a new culture** – which is driven by trust and results, you can’t control the time when your employees are at home

3. **Compliance** – to sustainably use the power of the cloud, you need to ensure security, resilience and compliance
Opportunities of change we see emerging from the crisis

- Empower and train your employees
- Transform your organisation
- Optimize your operations
- Transform your products
Ask us anything - Q&A

Instructions

In this Q&A, you as the audience can get involved, so please submit your questions for the Experts via the questions box on your left hand side.
Summary & key take-aways

What you should keep in mind

1. Make the transformation sustainable
   Reflect – Adopt – Integrate – Fix – Improve

2. Train people, close the knowledge gap
   Awareness – Educate – Skills – Certificate

3. Ensure security, regulatory compliance and data protection
   Manage Risk: Financial – Operational - Legal

➢ Despite all the potential we see, the value we created, the chances we see: To sustainably use the power of the cloud, we need to ensure security, resilience and compliance!

Cloud and Security: “What I need to do and what I should do…”

COMPLIANT Meets a specific standard at point in time (e.g. not negligent)
SECURE Lowers business risk to acceptable level by disrupting attacker return on investment (ROI)

LEVEL OF
ACCEPTABLE RISK
Thank you!

One Point of Contact:

Via our crisis helpline and PwC Switzerland website (EN | DE | FR)

Your experts:

Urs Küderli
Partner
Cybersecurity and Privacy
Email

Yan Borboën
Partner
Cybersecurity and Privacy
Email

Daniel Kubin
Cybersecurity and Cloud Expert
Cybersecurity and Privacy
Email
Thank you!