Office 365 risks map

SaaS

- **RS01** ●●● Spoofing and identity theft
- **RS02** ●●● Failure to control reversibility
- **RS03** ●●○ Poor identity and access management
- **RS04** ●●○ Uncontrolled data leakage
- **RS05** ●●○ Major change to features
- **RS06** ●●○ Network saturation following change in uses
- **RS07** ●○○ Data loss/corruption
- **RS08** ●○○ Service downtime

Development

PowerApps · PowerBi · Flow · Forms

- **RD01** ●●● Unprotected authentication secrets
- **RD02** ●●● Rights mismanagement
- **RD03** ●●● Incorrect OAuth setting
- **RD04** ●○○ Leakage through feature hijacking

Mail/Communication

Outlook · Yammer · Teams

- **RM01** ●●● Malicious message forwarding
- **RM02** ●●● O365 targeted social engineering (phishing)
- **RM03** ●●● Delegation not controlled by the user
- **RM04** ●●○ Email domain spoofing
- **RM05** ●●● Data leakage via a third-party service
- **RM06** ●●○ Use of legacy protocols (imap, pop3)
- **RM07** ●○○ Incorrect retention configuration

Workplace

Excel · Notes · PowerPoint · Word

- **RB01** ●●○ Malicious code execution
- **RB02** ●○○ Incompatibility after an update
- **RB03** ●●○ Data leakage due to advanced functions
- **RB04** ●○○ Uncontrolled complements

Collaboration

Teams · OneDrive · Sharepoint

- **RC01** ●●● Leakage through overly permissive sharing
- **RC02** ●●● Poor management of O365 groups
- **RC03** ●●○ Poor management of permissions on share
- **RC04** ●●○ Leakage through anonymous link sharing
- **RC05** ●●○ Spread of malicious files
- **RC06** ●○○ Use non-compliant with Charter

Tenant management

Office 365

- **RG01** ●●● Poor management of onboarding/ offboarding
- **RG02** ●●● Poor service governance
- **RG03** ●●● Loss of traceability of administrator actions
- **RG04** ●●● Non-segregation of administration
- **RG05** ●●● Lack of monitoring for privileged accounts
- **RG06** ●●○ Unfit administration team
- **RG07** ●●○ Administration from a compromised device
- **RG08** ●●○ Administrator error/ lack of awareness
- **RG09** ●●○ Poor Identity federation management (Azure AD)
- **RG10** ●●○ Poor Organizations's keys tenant management
- **RG11** ●●○ Not managing service control upgrades
- **RG12** ●●○ Poor management of guests's access rights

Legal

- **RL01** ●○○ Regulatory non-compliance

Devices

- **RA01** ●●● Use from a compromised device
- **RA02** ●●○ Use from a lost/stolen device
- **RA03** ●●○ Use from an uncontrolled device

Risk rating

- ●●● Likely/ High impact
- ●●○ Possible/ Medium impact
- ●○○ Unlikely/ Limited impact

CLUSIF

This infographic was taken from a Clusif working group (clusif.fr). It presents the risks associated with Office 365 but cannot be exhaustive.

Version june 2020