Strengthening your Cybersecurity with Cloudwork

Studentnet CLOUDWORK®

Make the cloud yours®

A little about me…

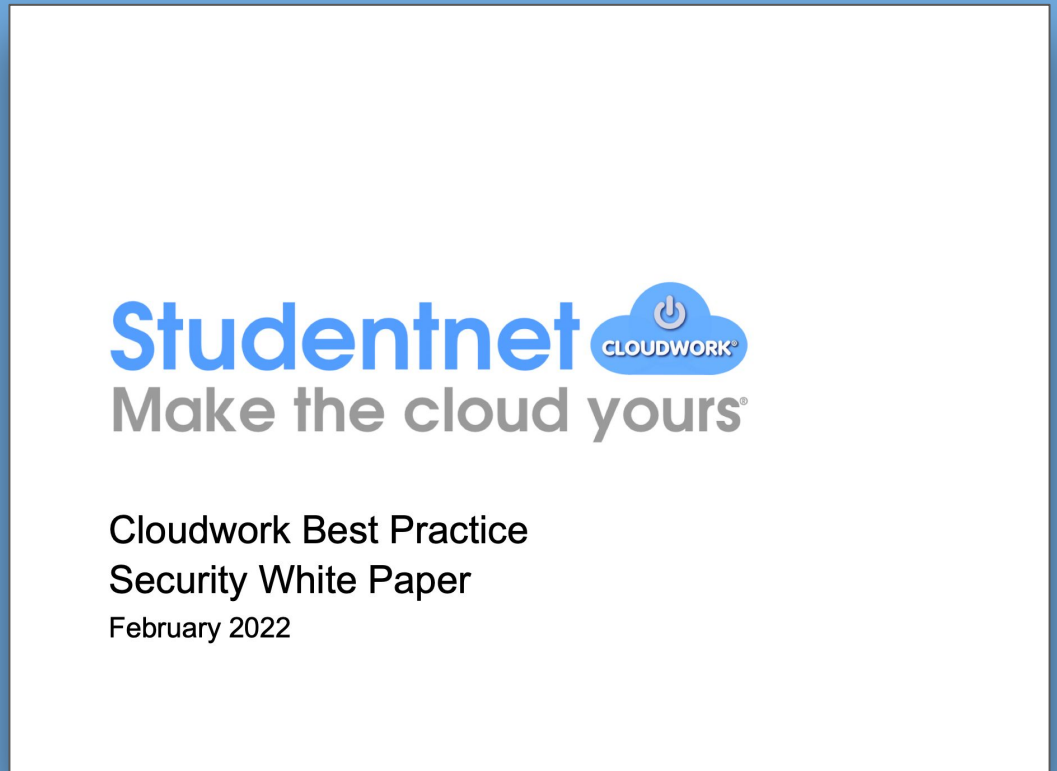
Consultant and Trusted Advisor

K-12 Technology Director

Risk and Compliance Executive

Reformed developer, sysadmin and DBA

Best Practice Security White Paper



Available at the end of this session


RISK

Risk is the effect of uncertainty on objectives


CYBER
SPACE
RISK

Cyber risk is the likelihood of a threat exploiting a vulnerability

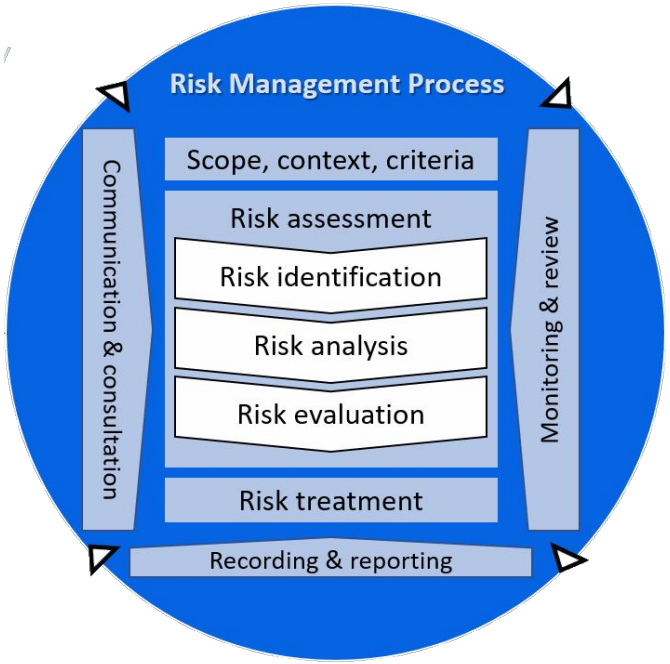
Information security is all about preserving:

1. **Confidentiality**
2. **Integrity**
3. **Availability**

A cyber-risk strategy, **appropriately resourced** and with **commitment from senior leadership**, will enables effective management of cyber risk through an ongoing process of **continuous improvement**, to protect the **confidentiality**, **integrity** and **availability** of information assets.

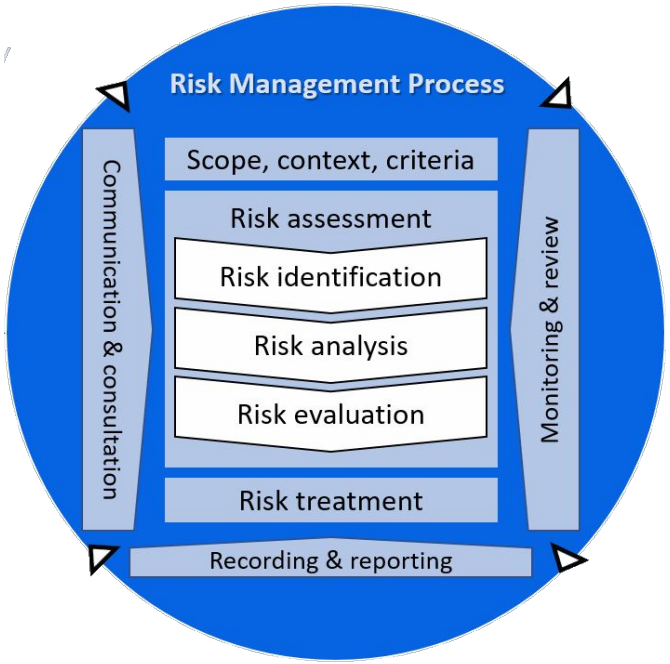
The Risk Management Process

1. Scope, context, criteria
    a. Who are your stakeholders?
    b. What data and systems do you have?
    c. What criteria will you use to assess risk?



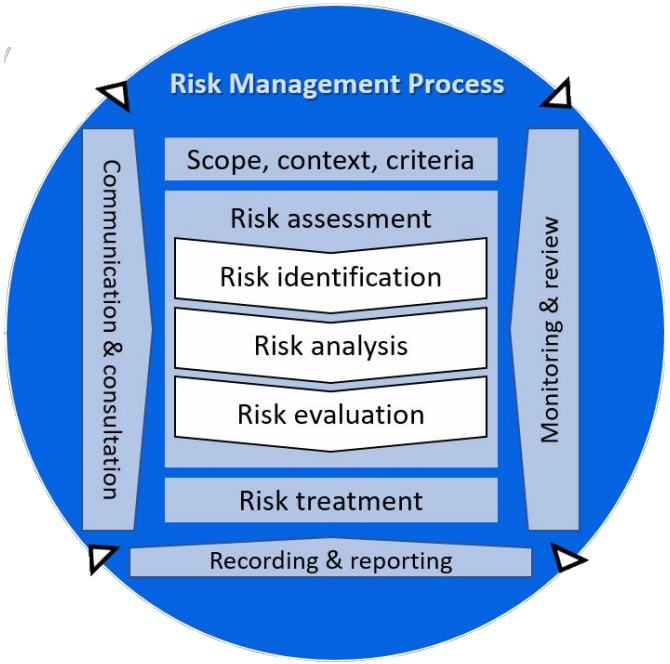
The Risk Management Process

1. Scope, context, criteria
    a. Who are your stakeholders?
    b. What data and systems do you have?
    c. What criteria will you use to assess risk?
2. Risk assessment
    a. Identify what could go wrong and why
    b. Analyse the likelihood and severity
    c. Evaluate the risk and your process



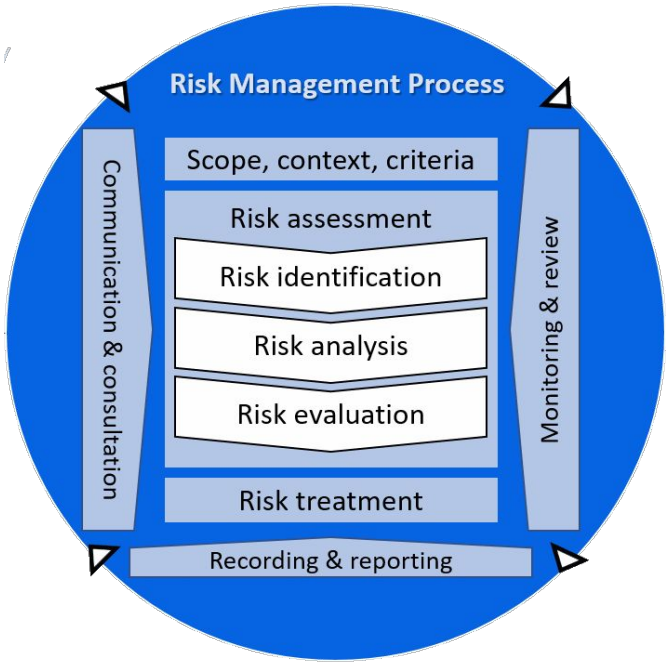
The Risk Management Process

1. Scope, context, criteria
    a. Who are your stakeholders?
    b. What data and systems do you have?
    c. What criteria will you use to assess risk?
2. Risk assessment
    a. Identify what could go wrong and why
    b. Analyse the likelihood and severity
    c. Evaluate the risk and your process
3. Risk treatment
    a. Implement measures (mitigations) to reduce the severity or likelihood of a risk (something going wrong)



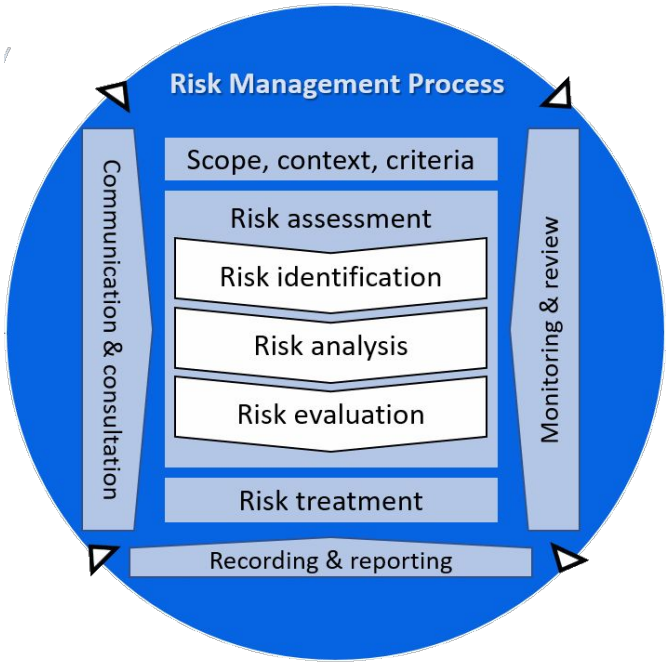
The Risk Management Process

1. Scope, context, criteria
    a. Who are your stakeholders?
    b. What data and systems do you have?
    c. What criteria will you use to assess risk?
2. Risk assessment
    a. Identify what could go wrong and why
    b. Analyse the likelihood and severity
    c. Evaluate the risk and your process
3. Risk treatment
    a. Implement measures (mitigations) to reduce the severity or likelihood of a risk (something going wrong)
4. Record and report to relevant stakeholders



The Risk Management Process

1. Scope, context, criteria
    a. Who are your stakeholders?
    b. What data and systems do you have?
    c. What criteria will you use to assess risk?
2. Risk assessment
    a. Identify what could go wrong and why
    b. Analyse the likelihood and severity
    c. Evaluate the risk and your process
3. Risk treatment
    a. Implement measures (mitigations) to reduce the severity or likelihood of a risk (something going wrong)
4. Record and report to relevant stakeholders
5. Communicate, consult, monitor and review to revise the process



When everything is important, nothing is important.

Severity risk criteria example

Catastrophic (5)	Multi-day outage of a key system and/or permanent loss of more than a week's worth of data and/or a data breach involving sensitive information for many individuals
Major (4)	A single day outage of a key system and/or permanent loss of more than a few day's worth of data and/or a data breach involving sensitive information for a small number of individuals or personal information for many individuals
Moderate (3)	A partial day outage of key systems and/or permanent loss of up to a day's worth of data and/or a limited data breach involving a small amount of personal information.
Minor (2)	Minor inconvenience for many users, loss or corruption of non-sensitive data
Insignificant (1)	No noticeable impact for users, no loss of data or system downtime

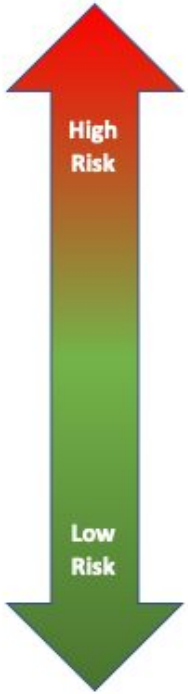
Risk criteria

Likelihood	Almost Certain (5)	Medium (5)	High (10)	Extreme (15)	Extreme (20)	Extreme (25)
	Likely (4)	Medium (4)	High (8)	High (12)	Extreme (16)	Extreme (20)
	Possible (3)	Low (3)	Medium (6)	High (9)	High (12)	Extreme (15)
	Unlikely (2)	Low (2)	Medium (4)	Medium (6)	High (8)	High (10)
	Rare (1)	Low (1)	Low (2)	Low (3)	Medium (4)	Medium (5)
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
		Severity				

Risk assessment

Risk	Severity	Likelihood	Mitigation Strategies	Residual Severity	Residual Likelihood	Final Rating
Staff member email account is compromised through a successful phishing attack, leading to a data breach	**Major**	**Almost Certain**	- Multi-factor authentication configured for all external services *- Simulated phishing / user awareness training bi-annually (planned)*	**Insignificant**	**Possible**	**Low**
Ex-employee or student gains unauthorised access to systems and data, resulting in a data breach	**Moderate**	**Possible**	- Automate de-provisioning of accounts with IDMS from HR and enrolment records with Cloudwork - Document procedures and training for human resources and enrolments staff	**Moderate**	**Rare**	**Low**

Tailoring controls to the level of risk



Systems

- Student management system
- Staff and student email
- Payroll and accounting systems
- Cloud storage
- Intranet
- Learning Management System
- Library platform
- Learning tools like Education Perfect, Mathletics
- Textbook platform

Cloudwork Controls

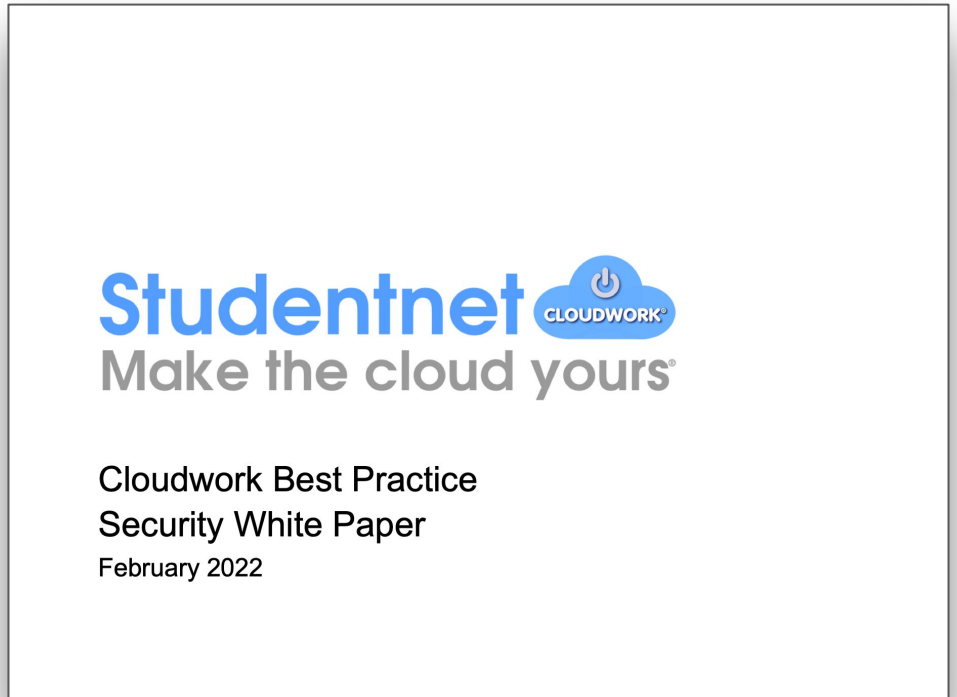
Prevent

- Multi-factor authentication
- Privileged identity management / delegation of access
- Authorisation rules
- Geoblocking

Detect and Respond

- Centralised logging, reporting and alerting
- Automated provisioning and deprovisioning of accounts

Where to begin?



1. Commitment from leadership
2. Plan the project
3. Risk assessment
4. Develop and implement your improvement plan
5. Review, report back and repeat!

Questions?