



smartWB

## Open training on eLearning with serious games

Milan Gocić, Milica Ćirić  
University of Niš

Training/ 15 June 2023

This project has been funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Thursday, 15<sup>th</sup> June 2023

In-person event

Moderators: Milica Ćirić, Milan Gocić, University of Nis (UNI)

First Session – Introduction

14:00-14:25	Digitalization in the water sector	Milan Gocić, UNI
14:25-14:35	Risks arising from digitalization	Milica Ćirić, UNI
14:35-14:45	Hacking the Water Supply: Florida Cyber Attack Explained <a href="https://www.youtube.com/watch?v=j_z9NmwqhHU">https://www.youtube.com/watch?v=j_z9NmwqhHU</a>	All participants

Second Session – Group work (GroupMap)

14:45-14:50	Group work introduction	Milica Ćirić, UNI
14:50-15:15	Group work – Identifying risks	All participants
15:15-15:25	Grouping and positioning risks	Milica Ćirić, UNI Milan Gocić, UNI All participants
15:25-15:50	Group work – Proposing actions and voting	All participants
15:50-16:00	Event evaluation and general conclusions	All participants



# Digitalization in the water sector

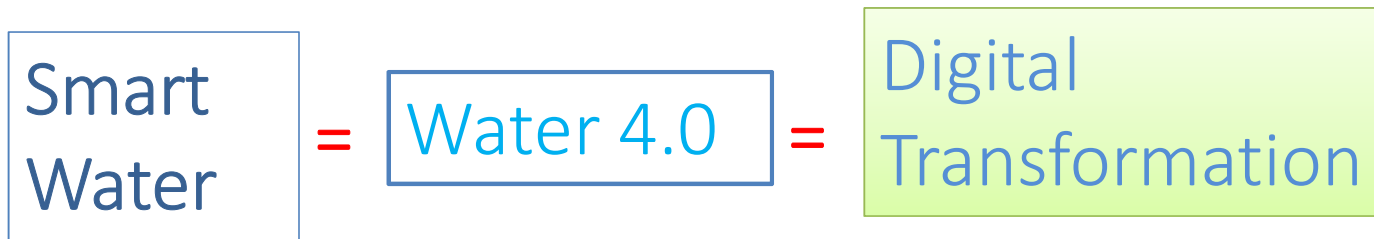
Milan Gocić  
University of Nis

## Trend in water infrastructures

Water infrastructures are **expensive** and **long lasting**.

Water infrastructures **cannot be replaced** as **frequently** as the evolution required.

**Digital Water is a key for this evolution.**



Smart Water is a reality and is no longer a choice. It is something that is just simply going to happen.



# Digitalization of water



Digitalization i.e. the use of digital technologies in day to day operations is reshaping the water sector and enabling urban services to seamlessly connect through their value chain.

Digitalization is transforming every sector of our society – from financial to education to natural resources, including how we plan our activities and how we communicate with each other.

This transition implies to increase resilience and sustainability of the water community.

The implementation of digital tools also creates new threats to infrastructure and service delivery systems, requiring new approaches to manage risks such as cyber security.



# Digitalization of water



Digitalization of water means adopting a smarter approach to water management.

Digitalization provide diversity and modularity combining concepts of water to achieve its usage purpose.

Digitalization represents an opportunity to better solve some of the more urgent issues utilities face.



## Digital technologies and water



There is a need for a fundamental change in the way we manage water.

Digital technologies offer unlimited potential to transform the water systems, helping water utilities to become **more resilient, innovative, efficient** and apply more economically viable strategies.

Digital solutions will be necessary for addressing the various problems utilities face to ensure adequate, reliable services to customers. Utilities need to take steps to strengthen the public health infrastructure to minimise the risk of the water crisis.

Using IoT technologies can help in integration and optimising of smart pumps, valves, sensors and actuators, enable „communication“ between water devices, and send real-time data that can be accessed and shared over the cloud.

To build a sustainable water future it is necessary **not only to have the adequate infrastructure, but also to control in advance what is going to happen and why.**



**KNOWING** our systems and our utilities

Providing **ANALYSES** and assisting  
**DECISION-MAKING**

Contributing to better decision  
**IMPLEMENTATION**

**MONITORING** the effects of decision  
implementation



# Water digitalization as a top priority for utilities in post-Covid world

Global mission should be to lead the change in building a Water Smart and Resilient world.

There is a need for understanding and discussion around the critical challenges in the water sector and how Smart water meters and how Digitalization of Water can lead to the future development of the water sector.

Handwashing and sanitization safety and health protocol under COVID-19 **increased a daily use of 20-40 litres** if per person cleans their hands at least 10 times a day instead of the average 5 times per day. This generates a **20-25% increasing in water demand, generation of wastewater from human settlements and additional pressure on overstretched water utilities.** Result would be **further exploitation of groundwater.**

Digitalization of water can be the greatest resolve for utility bodies to **fight the water stress and avoid Day Zero.**

## Drivers and objectives of water services and systems



We expect that our urban water systems ...  
... provide a good quality service for all, at all times  
... become more reliable, flexible, resilient, efficient, safe  
... play an effective role in circular economy

## Benefits of digital transformation for water utilities

- Data is translated into actionable information via **powerful analytical engines**, allowing end users to rapidly understand and act
- Managers can make better and accurate decisions for a resilient future by **combining simulation modeling or serious games with artificial intelligence methods**
- Water utilities can move towards a **customer-centric approach** thanks to technological innovations related to water meters
- Smart water approach in organizations generates greater efficiencies at a lower cost
- Digital solutions can help in the fight against Covid-19

Source: <https://smartwatermagazine.com/news/idrica/5-benefits-digital-transformation-water-utilities>

Digital water is **NOT AN OBJECTIVE**

Digital Water is a **MEANS** to better  
achieve our objectives

**UTILITIES MUST BE WISE**

A holistic digital roadmap should be built to set the beginning of the digital water. Global mission should be to lead the change in building a Water Smart and Resilient world.

**Digitalisation of water** and in general the water sector should help us to **mitigate a global water crisis** and to **build a more sustainable environment**.

New and advanced technologies should encourage changing the current status of water utilities.

**Digital solutions** are **not only a nice-to-have**, but a **must-have for water utilities** around the world.

Digital transformation automatically requires adequate cybersecurity as an inherent component of each water utility.

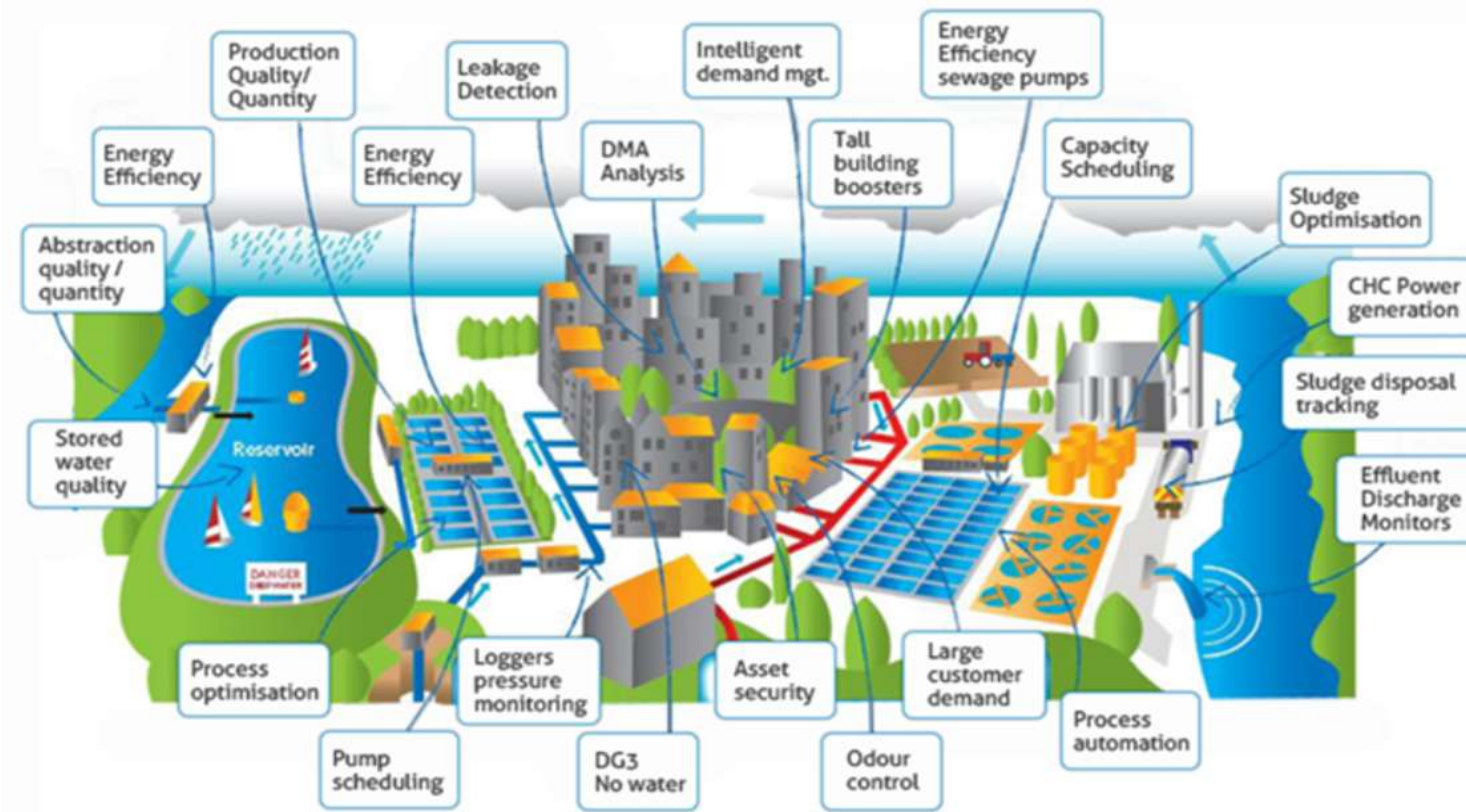
The benefits of digital transformation involve **higher transparency with citizens, companies and institutions**.

## Risks arising from digitalization

Milica Ćirić  
University of Nis

# smartWB

## An unavoidable development trend



Curricula innovation in climate-smart urban development based on green and energy efficiency with the non-academic sector

[www.smartwb.ucg.ac.me](http://www.smartwb.ucg.ac.me)



## BENEFITS OF DIGITALIZATION

- Real-time sensing and monitoring technologies can improve early leakage and water quality detection
- Maintenance action can be cost-effectively planned before functional failure thus reducing downtime and eliminating unexpected production stops
- Built-in intelligence results in adaptive behavior that assists in managing the effects of extreme weather conditions
- Experts can analyze data collected from sensors in order to determine optimal solutions for improving the operation of water and wastewater assets



## RISKS ARISING FROM DIGITALIZATION



Historically, the water utility control systems were not designed with security in mind, and while this alone doesn't make them vulnerable, considerations must be made when you're digitizing an existing system with older applications and tools.

Increasingly, there are threats around the critical control systems, especially those that control water flows, so treatment works and dams come to mind immediately as security and safety threats.



## RISKS ARISING FROM DIGITALISATION



- **Increased dependency on automation**
  - Risk of technical failures (no sensor works 24/7 & 365 days/year...)
  - Easier escalation from a single unit failure to system collapse
  - Do they make our operators less knowledgeable on processes?
  - Increased vulnerability of process stability
  - Increased risk of cascading effects between critical infrastructure (e.g. water and energy)
- **Causes**
  - System failures
  - Natural phenomena
  - Human errors
  - **Malicious actions – cyber attacks**
  - Third-party failures

## THE BIGGEST THREAT...



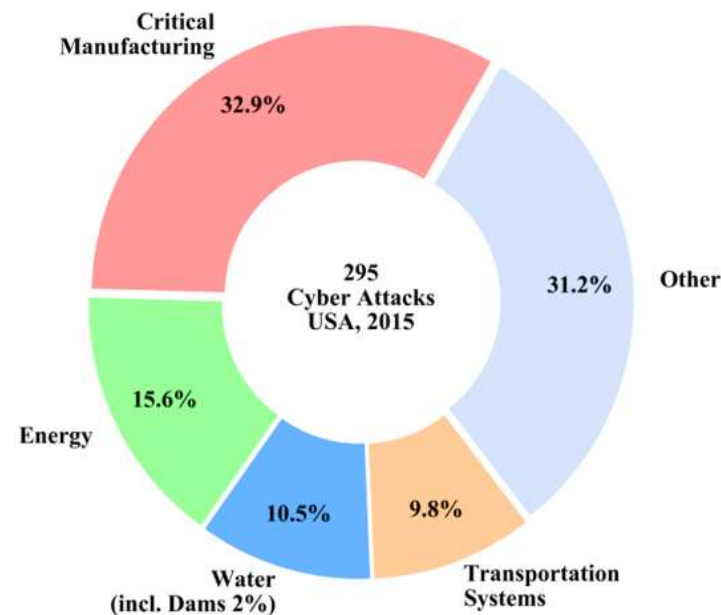
## Unpreparedness

Many water and wastewater utilities, particularly small systems, lack the resources for information technology (IT) and security specialists to assist them with starting a cybersecurity program. Utility personnel may believe that cyberattacks do not present a risk to their systems or feel that they lack the technical capability to improve their cybersecurity. Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security, cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization.

# smartWB THE ATTACKERS ARE ALSO INTERESTED IN THE WATER SECTOR



- Already a prominent target (**3rd most targeted**).
- Many cybersecurity incidents go either **undetected and unreported**, or undisclosed. (reputation+ customers trust)
- **Cyber security** is of course already part of the agenda for water companies.
- **Physical security** has been part of the agenda for some time.



*Cyber attack incidents in USA, 2015 (DHS, 2016)*

Cyber-attacks on water or wastewater utility business enterprise or process control systems can cause significant harm, such as:

- Upset treatment and conveyance processes by opening and closing valves, overriding alarms or disabling pumps or other equipment
- Deface the utility's website or compromise the email system
- Steal customers' personal data or credit card information from the utility's billing system
- Install malicious programs like ransomware, which can disable business enterprise or process control operations.

These attacks can: compromise the ability of water and wastewater utilities to provide clean and safe water to customers, erode customer confidence, and result in financial and legal liabilities.

- **Malware** – Malicious software variants—such as worms, viruses, Trojans, and spyware—that provide unauthorized access or cause damage to a computer.
- **Ransomware** – A type of malware that locks down files, data or systems, and threatens to erase or destroy the data - or make private or sensitive data to the public - unless a ransom is paid to the cybercriminals who launched the attack.
- **Phishing / social engineering** – Form of social engineering that tricks users into providing their own PII or sensitive information.
- **Insider threats** – Current or former employees, business partners, contractors, or anyone who has had access to systems or networks in the past can be considered an insider threat if they abuse their access permissions.
- **Distributed denial-of-service (DDoS) attacks** – Attempts to crash a server, website or network by overloading it with traffic, usually from multiple coordinated systems.
- **Advanced persistent threats (APTs)** – An intruder or group of intruders infiltrate a system and remain undetected for an extended period. The intruder leaves networks and systems intact so that the intruder can spy on business activity and steal sensitive data while avoiding the activation of defensive countermeasures.
- **Man-in-the-middle attacks** - An eavesdropping attack, where a cybercriminal intercepts and relays messages between two parties in order to steal data.

- Keep everything up to date (anti-virus, security patches...)
- Set up automatic backups of critical systems to use as restore files
- Implement rigorous user authentication (multi-factor authentication, unique accounts and passwords, restricted privileges)
- Restrict internet access
- Separate process control system traffic from business traffic
- Eliminate and/or restrict remote access
- Assess vulnerabilities in all critical IT systems



## BEST PRACTICES FOR MINIMIZING WEAKNESSES AND PREVENTING ATTACKS

- Keep an inventory of control system devices and ensure this equipment is not exposed to networks outside the utility
  - Never allow any machine on the control network to “talk” directly to a machine on the business network or on the Internet.
- Segregate networks and apply firewalls
  - Classify IT assets, data, and personnel into specific groups, and restrict access to these groups.
- Use secure remote access methods
  - A secure method, like a virtual private network, should be used if remote access is required.
- Establish roles to control access to different networks and log system users
  - Role-based controls will grant or deny access to network resources based on job functions.
- Require strong passwords and password management practices
  - Use strong passwords and have different passwords for different accounts.

## BEST PRACTICES FOR MINIMIZING WEAKNESSES AND PREVENTING ATTACKS

- Stay aware of vulnerabilities and implement patches and updates when needed
  - Monitor for and apply IT system patches and updates.
- Enforce policies for the security of mobile devices
  - Limit the use of mobile devices on your networks and ensure devices are password protected.
- Have an employee cybersecurity training program
  - All employees should receive regular cybersecurity training.
- Involve utility executives in cybersecurity
  - Organizational leaders are often unaware of cybersecurity threats and needs.
- Monitor for network intrusions and have a plan in place to respond
  - Be capable of detecting a compromise quickly and executing an incident response plan.

### Utility

- Disconnect compromised computers
- Notify IT experts
- Assess damage to utility systems and equipment
- Execute the utility Emergency Response Plane (ERP)

### IT Experts

- Review logs, take a “forensic image” of the affected IT system
- Identify if employee or customer identifiable information was compromised

### Utility

- Collaborate with IT experts
- Notify employees and customers if PII was compromised
- Create an after action report (AAR) and an improvement plan (IP) based on the AAR

### IT Experts

- Remove malware, corrupted files and other changes to IT systems and restore IT systems
- Install patches and updates and perform other countermeasures to harden the system against exploited vulnerabilities



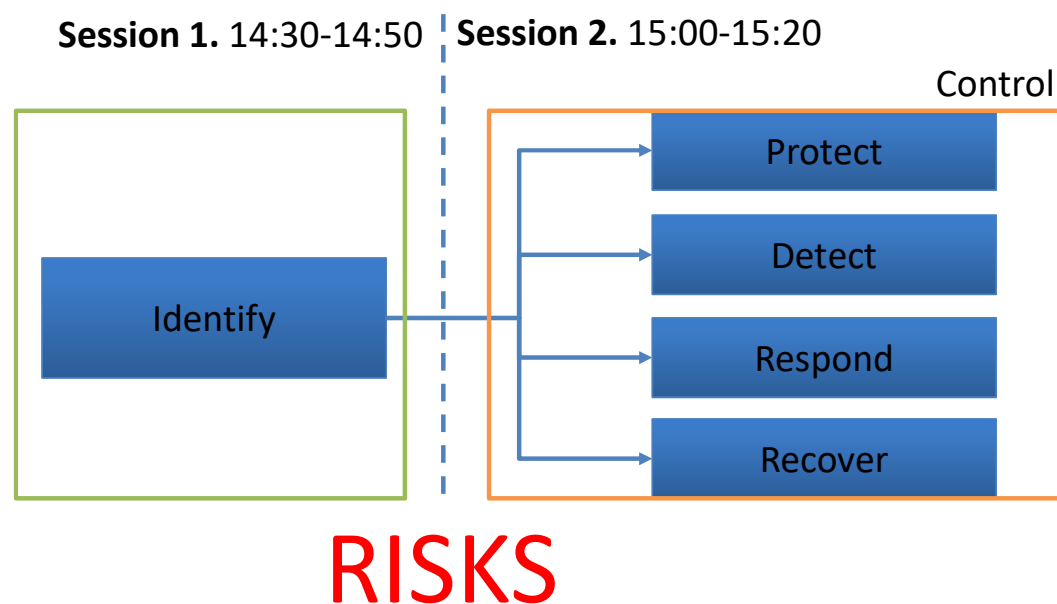
## TOP THREE ADVICES FOR CYBERSECURITY IN WATER SECTOR



Co-funded by  
the European Union

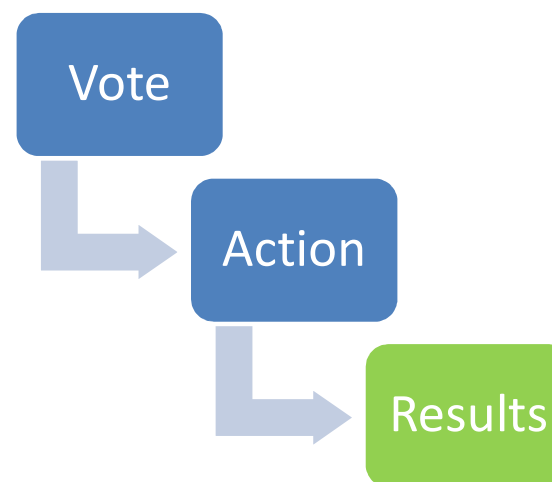
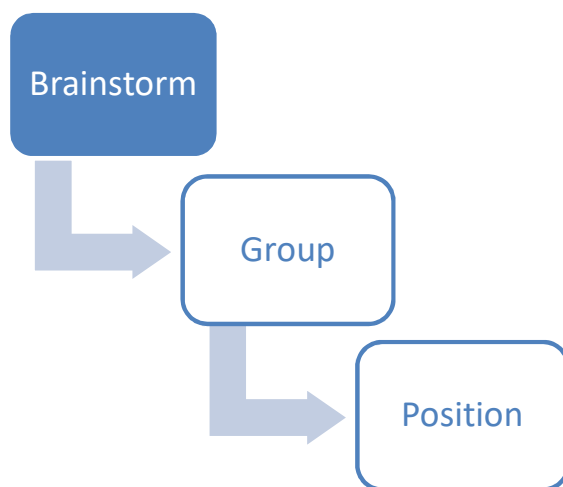
- Be aware of the risks
- Try to prevent attacks
- Prepare recovery measures for post-attack





**Session 1. 14:30-14:50**

**Session 2. 15:00-15:20**







Browse to [join.groupmap.com](https://join.groupmap.com)  
and enter invite code

**C82-A4F-77A**

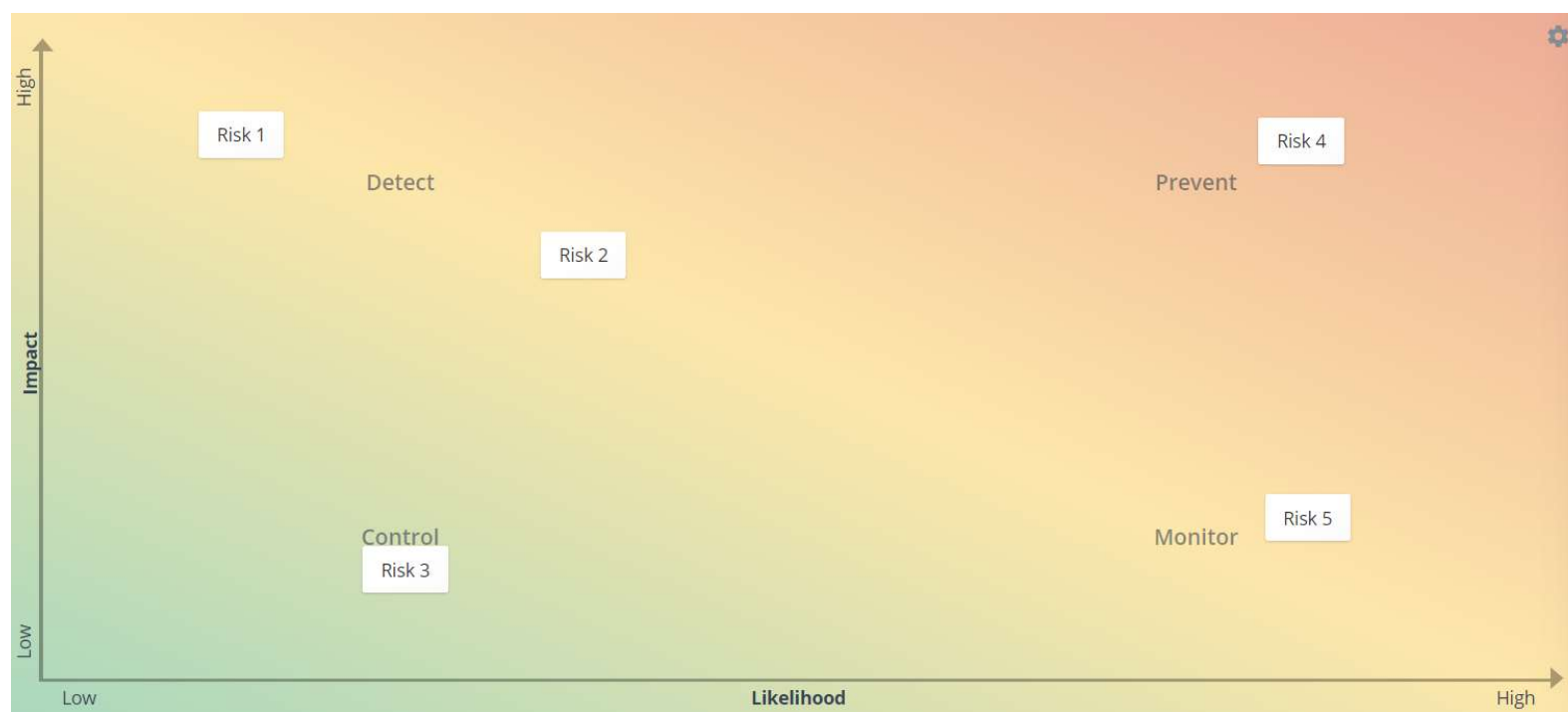
or go to link

<https://join.groupmap.com/C82-A4F-77A>

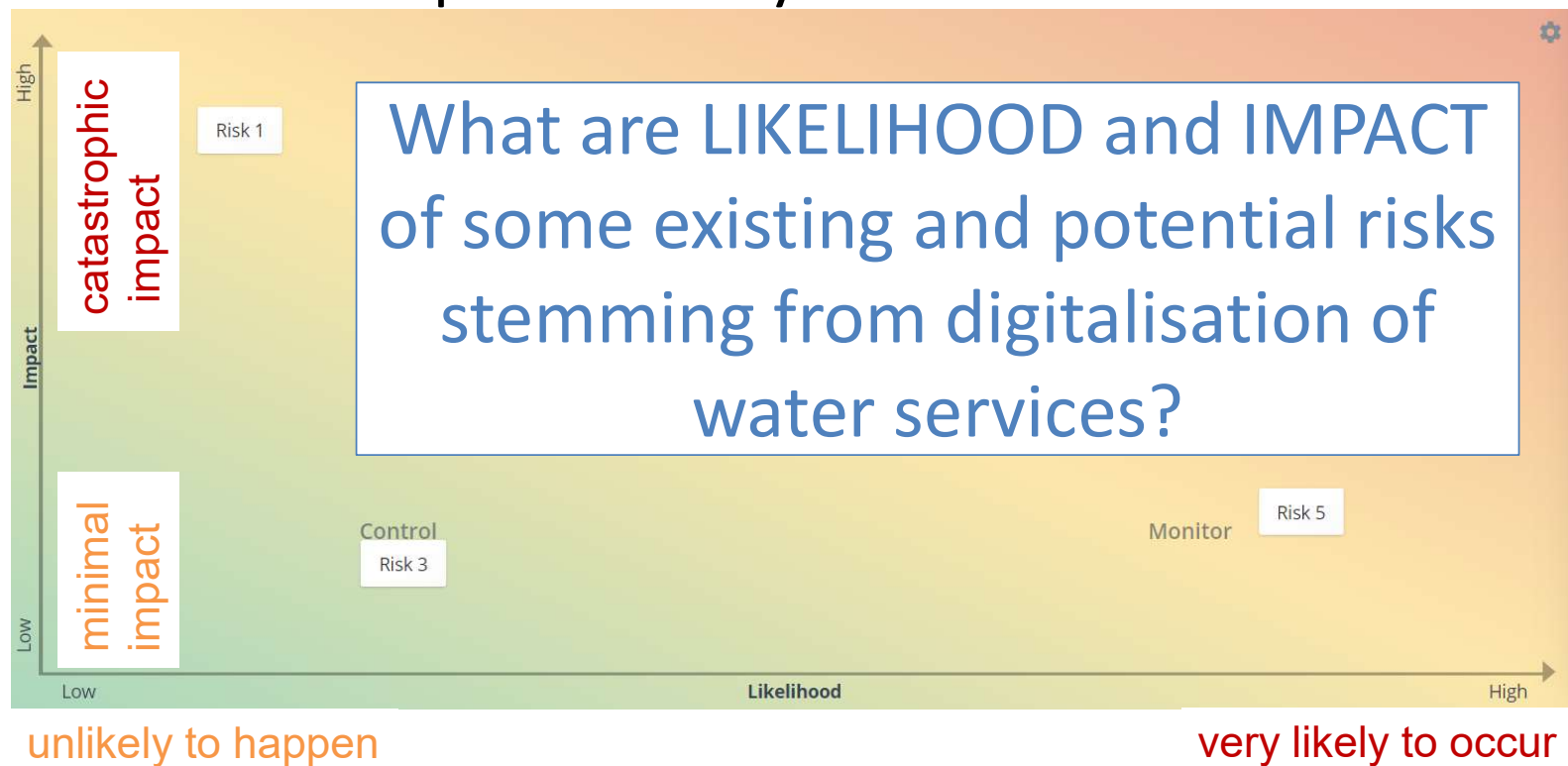
### Risks landscape

IMPACT	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Low	Medium
		Low	Medium	High
		LIKELIHOOD		

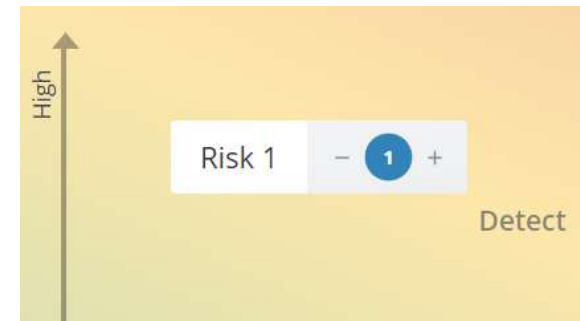
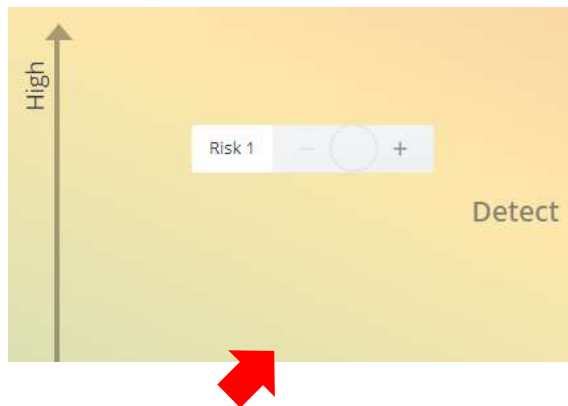
Click on the landscape and add your ideas



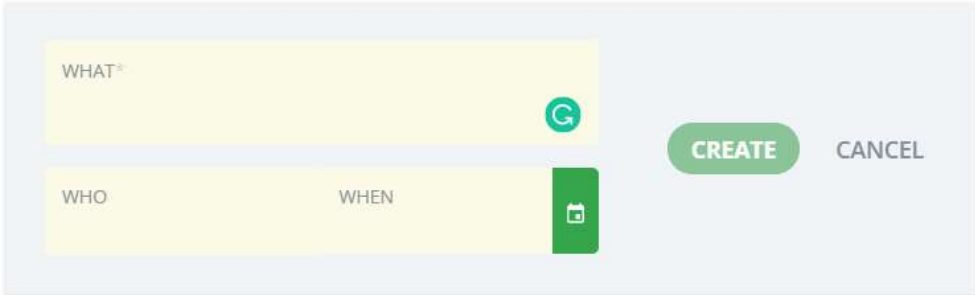
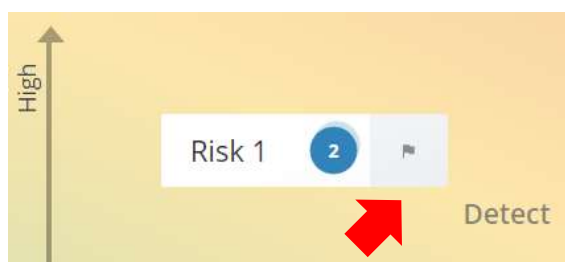
Click on the landscape and add your ideas



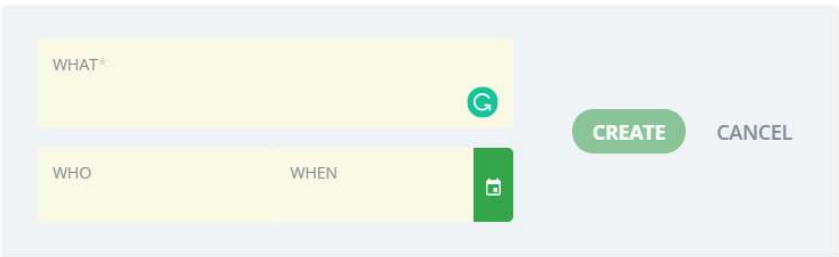
- You have **4 votes**
- You can put multiple votes



## SUGGEST ACTIONS

A form for suggesting actions. It has two input fields: "WHAT\*" and "WHO". The "WHAT\*" field has a green circular icon with a "G" inside. The "WHO" field has a green square icon with a calendar icon inside. To the right of the fields are two buttons: "CREATE" and "CANCEL".

## SUGGEST ACTIONS

A screenshot of the "SUGGEST ACTIONS" form. It has a light blue background. The form contains three input fields: "WHAT\*" (with a green circular icon containing a 'G'), "WHO", and "WHEN" (with a green calendar icon). To the right of the fields are two buttons: "CREATE" (green) and "CANCEL" (light blue).

- **WHAT** should be done (regulations, standards, technical measures etc.)
- **WHO** should do it (government, researchers, treatment plants etc.)
- **WHEN**: short term, long term or a specific date

Protect

Detect

Respond

Recover



Please follow the link to the evaluation form.  
Thank you for participating!!!

<https://forms.gle/9jLfQSvxx8vKRcKC6>