2024

WF 1.0 INDEX

A modern risk index designed to simplify reporting of potential organizational threats to private businesses.

PREPARED BY WF COMMAND CENTER

FOR PUBLIC COMMENT

Executive Summary

The WF Index 1.0 is a quick tool for executives to gauge cybersecurity posture, prioritize responses, and guide strategic planning. It aligns with cybersecurity by helping identify vulnerabilities, mitigate threats, and enhance resilience against cyber attacks.

Overview

In today's cloud-age environment, identifying and managing cyber risks is crucial to private businesses' stability and future growth. This ensures organizations protect their assets, maintain operational resilience, and retain stakeholder trust. To assess the potential impact of these risks, the Waffle House Risk Index 1.0 (WF 1.0) is designed to simplify the categorization, mapping, and communication associated with the process.

The Waffle House Risk Index adapts the original index's familiar but informal color-coded system to categorize the severity and impact of cyber risks. It consists of three levels: Green, Yellow, and Red, each indicative of varying degrees of risk severity and impact on cybersecurity. This also includes the addition of a new Gray status to indicate unmapped risks that are just emerging.

Scope and limitations

- Green (Low Severity, Low Impact): Indicates routine operations with no immediate threats or disruptions to the organization, its services, or solutions. Security measures are effective, and no significant incidents are detected.

- Yellow (Moderate Severity, Moderate Impact): Highlights challenges affecting organizational operations, such as minor incidents or emerging threats that require attention but are manageable with existing controls.

- Red (High Severity, High Impact): Signals severe disruptions or incidents with significant impact on the organization, such as major data breaches, widespread malware outbreaks, or critical infrastructure failures.

Methodology

The Waffle House Risk Index 1.0 is developed by adapting the original Waffle House Index to the domain of cybersecurity. The index was created through a collaborative process involving cybersecurity experts, risk management professionals, and executive stakeholders. The following steps were taken to create the index:

Identifying Key Risk Factors: We identified key factors contributing to cybersecurity risks, such as the severity of potential incidents, the impact on business operations, and the effectiveness of existing security measures.

Defining Color-Coded Levels: We established three color-coded levels - Green, Yellow, and Red - to represent varying degrees of risk severity and impact. Each level was defined based on the potential impact of incidents on operations and the organization's overall security posture.

Mapping to Existing Frameworks: We mapped the color-coded levels of the index to established cybersecurity frameworks, such as ISO/IEC 27001, NIST Cybersecurity Framework, and SOC 2, to ensure alignment with industry best practices and standards.

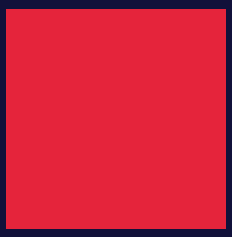
Validation and Feedback: The index is now being reviewed, by you, to validate by subject matter experts and stakeholders to ensure its relevance, accuracy, and usability in real-world cybersecurity scenarios.

#	Questions
1.	What is the current state of our cybersecurity posture?
2.	Which cyber risks require immediate attention and response?
3.	How should resources be allocated to mitigate cyber risks effectively?
4.	Are our cybersecurity strategies and controls effective in mitigating potential risks?
5.	How do external factors impact our cybersecurity posture?
6.	What is the likelihood of a cyber incident causing disruption to critical business operations?
7.	How does our cybersecurity posture compare to industry benchmarks or peer organizations?

WF Risk Index 1.0

Color Coded Risk Rating System

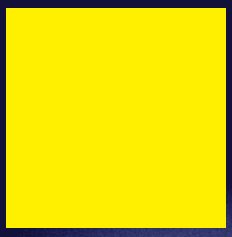
There are four color ratings used to delineate the level of severity, impact, and plausibility a risk may pose to an organization.



RED

Significant disruptions requiring immediate and extensive action.

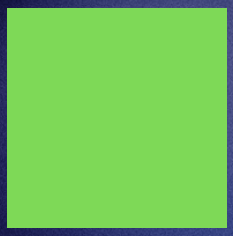
- Major supply chain disruptions affecting key resources.
- Serious cybersecurity breach compromising sensitive data.



YELLOW

Some challenges affecting operations, but recovery is manageable.

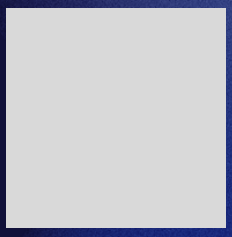
- Limited disruption with potential supply chain delays.
- Minor incidents with data security measures in place.



GREEN

No immediate threats or disruptions to operations.

- Routine operations with no supply chain disruptions.
- No significant cybersecurity incidents or data breaches.



GRAY

New emerging threat detected that has yet to be evaluated

- Risk can range from zero-day to midnight brawl.
- High likelihood of burnt toast, but it may be just right.

Mapping Risks

Factors for Mapping Color Status

By evaluating three key factors - the severity of potential impact, the probability of occurrence, and the effectiveness of existing controls - organizations can accurately map risk statuses using the Waffle House Risk Index for Cyber Risks. This strategy allows for a thorough assessment of cybersecurity risks, facilitating informed decision-making and prioritizing response efforts.

Key Indicator	Action	Factors
Severity of Potential Impact:	Impact risk could have on business operations	• Data loss • Disruptions • Financial loss
Likelihood of Occurrence	Probability of the risk materializing into an actual incident or disruption	• Historical data • Threat intel • Vuln assessments • Emerging trends
Effectiveness of Existing Controls	Effectiveness of existing controls and mitigation measures in mitigating the risk	• Security posture • Control environment • IR capabilities • Resilience measures

Example Mapping

Example chart that maps the severity of potential impact, likelihood of occurrence, and effectiveness of existing controls to a data breach risk:

Risk Factor	Low	Medium	High
Severity of Potential Impact	Minimal impact on business operations. Limited data exposure with low financial and reputational consequences.	Moderate impact on business operations. Moderate data exposure with potential financial and reputational consequences.	Severe impact on business operations. Extensive data exposure with significant financial and reputational consequences.
Likelihood of Occurrence	Low probability of occurrence due to robust cybersecurity measures, regular monitoring, and proactive risk management.	Moderate probability of occurrence due to some vulnerabilities or emerging threats, but with adequate controls in place to mitigate risks.	High probability of occurrence due to significant vulnerabilities, exploitation of known weaknesses, or targeted cyber attacks. Controls may be inadequate or ineffective.
Effectiveness of Existing Controls	Strong cybersecurity controls in place, including encryption, access controls, and regular security audits. Incident response plan is well-documented and regularly tested.	Some cybersecurity controls in place, but gaps or weaknesses exist, such as outdated software or insufficient employee training. Incident response plan may lack maturity or testing.	Limited or ineffective cybersecurity controls in place. Lack of encryption, access controls, or monitoring. Incident response plan may be non-existent or poorly developed.

Scenario Mapping

This chart shows varying levels of severity based on the following scenario: It's 2 AM, all the alcohol in your system has evaporated after being at a Foo Fighters concert, and now you are hungry. What is the likelihood you will see a fight at WF?

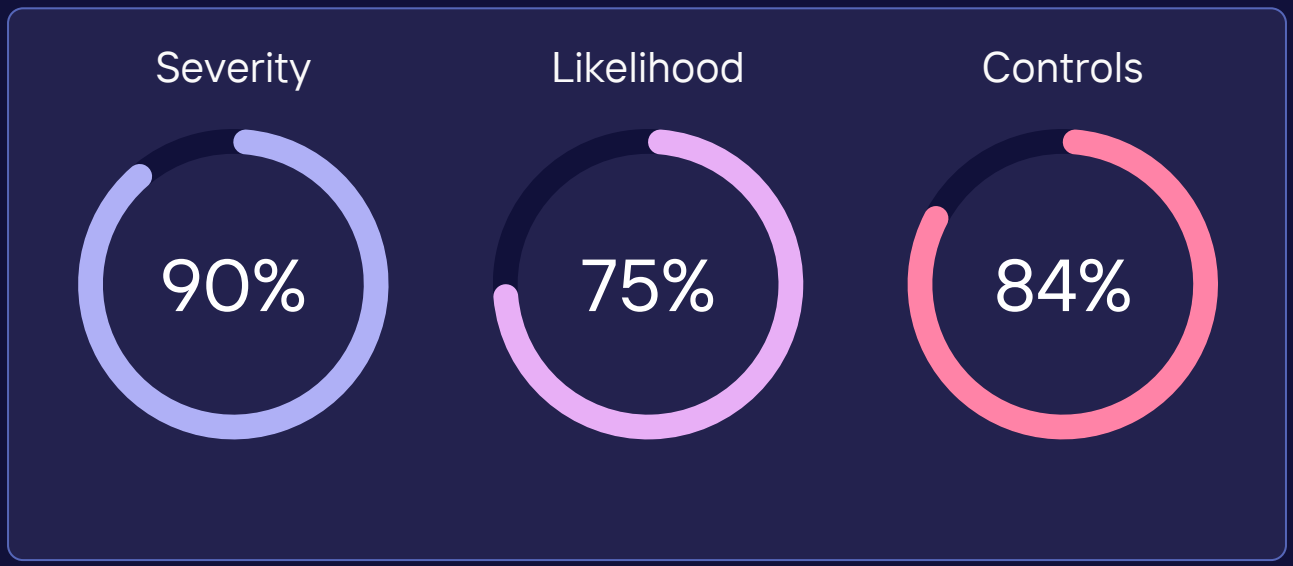
Risk Factor	Low	Medium	High
Severity of Potential Impact	If you see a fight, there will be no impact to you, but it may be a blast.	If you are involved in the fight, there is a good chance the cook will slap you.	If you start the fight there is a high probability of getting knocked out and/or going to jail.
Likelihood of Occurrence	There is a low probability you will start the fight.	There is a medium probability you will start the fight.	There is a high probability you will start the fight.
Effectiveness of Existing Controls	You only had a Zima, you ate prior, and had some water.	You are essentially hungover, but you ate prior and had some water.	You are essentially hungover, you failed to eat before the concert, and water was $5.

Red

Scenario: Significant disruptions requiring immediate and extensive action.

Risk Examples:

- A major hurricane hits a region where the company has a data center, causing widespread power outages and impacting data access and services.
- A global supply chain disruption occurs due to geopolitical events, severely affecting the availability of critical components for the company's products.
- A sophisticated cyber attack results in a significant data breach, leading to the compromise of sensitive customer information.
- A major infrastructure failure, such as a catastrophic server malfunction, results in a widespread service outage affecting a large customer base.

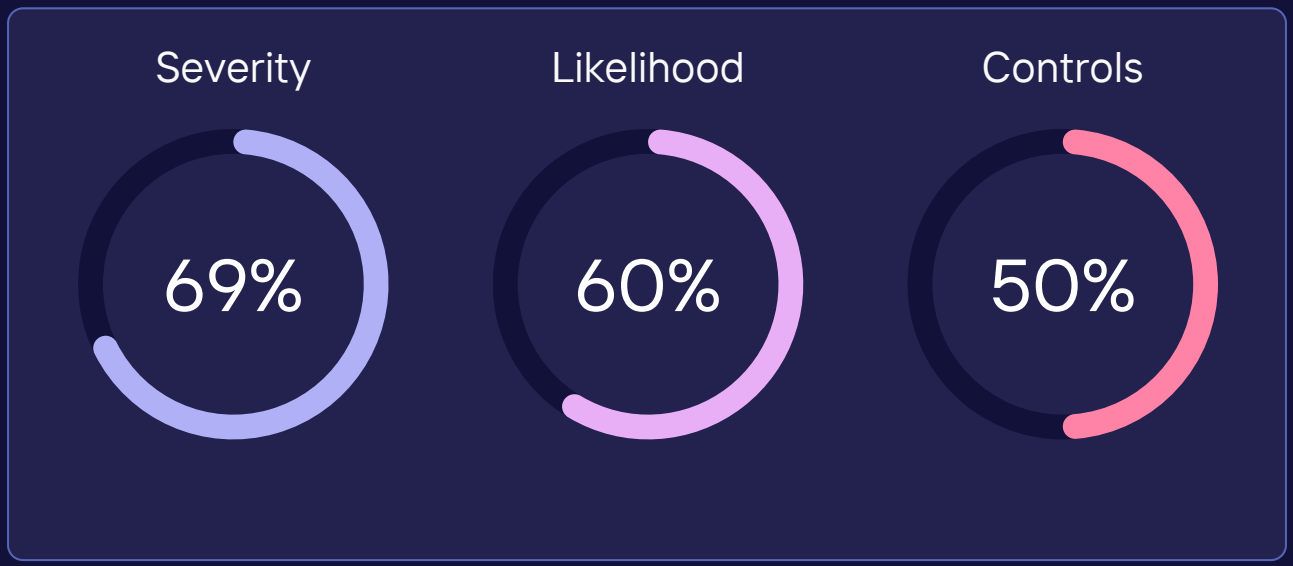


Yellow

Scenario: Some challenges affecting operations, but recovery is manageable.

Risk Examples:

- A moderate earthquake occurs in a region where the company has an office, causing temporary disruption to local operations.
- A key supplier experiences delays in delivering essential hardware components, impacting production timelines.
- An isolated cybersecurity incident, such as a phishing attack, is detected and mitigated before causing extensive damage.
- Scheduled maintenance on critical infrastructure results in temporary service interruptions that are quickly addressed.

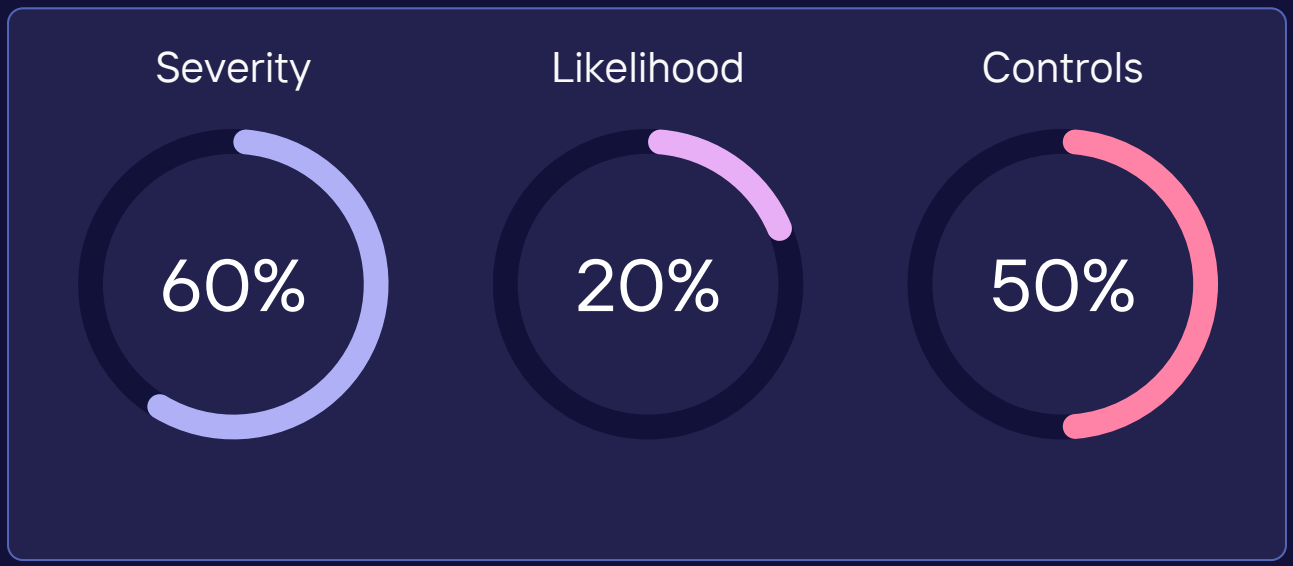


Green

Scenario: Routine operations with no immediate threats or disruptions.

Risk Examples

- Regular day-to-day activities with no significant weather events or natural disasters in the company's geographical areas of operation.
- Supply chain is stable, and key vendors are meeting delivery expectations.
- Ongoing cybersecurity measures effectively prevent any major incidents or breaches.
- All critical systems are functioning optimally.



Standard Mappings

WF Risk Index 1.0 Vs. NIST CSF

Mapping the three color-coded levels of the Waffle House Index to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) functions simplifies risk communication to superiors. The NIST CSF revolves around five core functions: Identify, Protect, Detect, Respond, and Recover.

1. Green (Low Severity, Low Impact):

- NIST CSF Functions:Identify: Routine identification of assets, risks, and dependencies.
- Protect: Ongoing protection measures to maintain the integrity of systems and data.
- Detect: Continuous monitoring for any potential anomalies or threats.
- Respond: Well-defined response procedures for routine incidents.
- Recover: Regularly tested recovery processes for minor disruptions.

2. Yellow (Moderate Severity, Moderate Impact):

- NIST CSF Functions:Identify: Identification of moderate-level risks and challenges.
- Protect: Additional protective measures activated to mitigate moderate-level threats.
- Detect: Enhanced monitoring and detection capabilities for moderate incidents.
- Respond: Coordinated response efforts for moderate disruptions.
- Recover: Recovery plans adjusted to address moderate-level impact.

3. Red (High Severity, High Impact):

- NIST CSF Functions:Identify: Swift and thorough identification of high-impact risks.
- Protect: Immediate activation of high-impact protective measures.
- Detect: Rapid detection and response to high-severity incidents.
- Respond: Emergency response procedures executed to mitigate the impact of severe disruptions.
- Recover: Intensive recovery efforts with a focus on restoring critical systems and services.

In this mapping, the Waffle House Risk Index color-coded levels align with the NIST CSF functions to provide a cybersecurity-oriented perspective. The NIST CSF is a comprehensive framework that helps organizations manage and improve their cybersecurity posture, and the Waffle House Index can complement it by offering a quick and visual way to assess the overall operational resilience and impact of events on a broader scale. Both frameworks aim to enhance an organization's ability to identify, protect, detect, respond to, and recover from various challenges, whether they be related to cybersecurity or broader operational risks.

Standard Mappings

WF Risk Index 1.0 Vs. ISO 27001

Mapping the three color-coded levels of the Waffle House Index to the clauses of the ISO/IEC 27001 standard, which is a widely recognized global standard for information security management systems (ISMS), adds some international flavor to the approach.

1. Green (Low Severity, Low Impact):

- ISO 27001 Clauses:Context of the Organization (Clause 4): Establishing the context, including the organization's external and internal issues.
- Leadership (Clause 5): Leadership's commitment to the ISMS and ongoing support for information security.
- Planning (Clause 6): Routine planning and risk assessment activities for information security.
- Support (Clause 7): Routine provision of resources and training to support information security.

2. Yellow (Moderate Severity, Moderate Impact):

- ISO 27001 Clauses:Operation (Clause 8): Implementing information security controls and measures to address moderate-level risks.
- Performance Evaluation (Clause 9): Monitoring and evaluating the performance of information security controls in response to moderate incidents.

3. Red (High Severity, High Impact):

- ISO 27001 Clauses:Performance Evaluation (Clause 9): Intensive monitoring and evaluation in response to high-impact incidents.
- Improvement (Clause 10): Taking corrective actions and continuously improving the ISMS to address severe disruptions.
-

In this mapping, the Waffle House Risk Index color-coded levels align with the clauses of ISO/IEC 27001 to provide a framework for managing information security risks. ISO 27001 focuses on a systematic approach to information security, and the Waffle House Risk Index can be seen as a way to quickly assess the severity of potential disruptions and incidents that may impact the overall information security management system.

The integration of the Waffle House Index with ISO 27001 can help organizations prioritize and tailor their information security measures based on the perceived impact and severity of events, ensuring a flexible and adaptive approach to maintaining the confidentiality, integrity, and availability of information assets.

-

Framework Mappings

WF Risk Index 1.0 Vs. SOC 2

SOC 2 (Service Organization Control 2) is a framework for managing and securing sensitive information for service providers. It focuses on five "Trust Service Criteria": Security, Availability, Processing Integrity, Confidentiality, and Privacy. Here is how to map the Waffle House Risk Index color-coded levels to the key aspects of SOC 2 criteria:

1. Green (Low Severity, Low Impact):

- SOC 2 Criteria:Security: Routine security measures and controls are in place to protect sensitive data.
- Availability: Regular operations with no significant disruptions to service availability.

2. Yellow (Moderate Severity, Moderate Impact):

- SOC 2 Criteria:Security: Additional security measures activated to address moderate-level risks.
- Availability: Measures in place to mitigate the impact of moderate disruptions, ensuring services remain available.

3. Red (High Severity, High Impact):

- SOC 2 Criteria:Security: Immediate activation of high-impact security controls in response to severe incidents.
- Availability: Intensive efforts to restore and maintain service availability during high-impact disruptions.

In the context of SOC 2, the Waffle House Risk Index color-coded levels align with the key Trust Service Criteria to indicate the impact and severity of potential disruptions on the security, availability, and overall trustworthiness of services provided by the organization. The SOC 2 framework, like ISO 27001, emphasizes a systematic approach to managing risks and ensuring the security and privacy of sensitive information.

The integration of the Waffle House Risk Index with SOC 2 can help organizations tailor their security and availability measures based on the perceived impact of events, ensuring alignment with the specific criteria and controls outlined in the SOC 2 framework. This approach allows organizations to communicate their commitment to security and reliability to their clients and stakeholders.

-

Sample Risk Report

The following sample risk report is designed to more easily communicate documented and emerging risks. Replace the fill copy prior to sending this as an internal memo or increase the risks of being laughed at.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus condimentum nunc ligula nec tempor porttitor. Phasellus fermentum at imperdiet ut, eu semper volutpat, ex non fringilla.

Aenean vel tellus at quam ultrices fringilla. Integer pretium nunc non consectetur sed sodales. Proin lorem nisl, fermentum at imperdiet ut, tincidunt et leo. Pellentesque urna est, ornare pretium.

Next steps

#	Recommendations	Priority
1	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus condimentum nunc ligula nec tempor porttitor. Phasellus fermentum at imper-diet ut, eu semper volutpat	
2	Suspendisse eget ipsum nunc. Curabitur sit amet libero non nibh rhoncus viverra ut dictum sem. Donec scelerisque non ex sit amet ornare.	
3	Duis cursus metus quam, nec scelerisque leo sollicitudin in. Ut condimentum vestibulum odio. Phasellus eleifend et est sit amet lacinia.	
4	Suspendisse nulla lorem, semper et nibh ut, pulvinar tristique urna. In auctor magna id ipsum vestibulum egestas.	

WF 1.0 INDEX

To provide your input on this public draft, please go here. This is a very real draft report and not at all tied to April 1, 2024.