aws User Group Ljubljana

Getting Started with NIS2: Navigating Cybersecurity Compliance

Marko Ličina

28.11.2024

aws User Group Ljubljana

1811 SOLUTIONS

About me:

- I've worked in IT for a long time and in almost every technical or sales role, except as a developer.
- Currently, I run my own business, focusing on providing services and products related to cybersecurity and NIS-2 compliance.
- I believe in continuous learning and enjoy exploring and discovering new things.
- I am currently working hard to improve my knowledge of NIST and ISO/IEC frameworks.

Webpages and links:

NIS-2 : https://www.nis-2.pro

1811SOLUTIONS: https://www.1811solutions.eu

LinkedIn: https://www.linkedin.com/in/markolicina

Save me as Contact :

QR Code Disclaimer:
The QR codes included in this presentation are **safe**, **clean**, and do not pose any security risks. They are provided solely for easy access to relevant information and resources.

Disclaimer:
I am in no way associated with **ENISA** (European Union Agency for Cybersecurity) or any Slovenian agency. This presentation is provided **"as is"** and does not represent their views.
The content reflects my own perspectives, developed by following best practices, recognized frameworks (such as the NIST 800 Series and the ISO 27000 Family), and publicly available information provided by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and frameworks like the USA Federal Information Security Management Act (FISMA) —organizations with extensive experience in business continuity and disaster recovery.

Why should you care about NIS-2?

- **This could be/is probably the biggest IT project of 2025,and must be treated as such with budgeting and planning for done sooner rather than later!!!**
- **Supply Chain Impact (Suppliers to NIS 2 Entities)**: Even if your organization is not directly affected, being a supplier to a regulated entity will require compliance and you could be subject to audits!
- **High Penalties**: Companies will be audited. Non-compliance can result in fines of up to **€10 million** or **2% of global turnover**.
- **Management Responsibility:** Management is directly accountable for non-compliance and faces penalties for negligence.
- **Opportunity for Growth:** Compliance can improve cybersecurity posture, build customer trust, and provide a competitive edge.
- **Broader Scope:** NIS-2 expands its coverage to include more sectors and organizations, increasing the likelihood your business is affected.
- **Stricter Requirements:** Introduces stricter obligations for cybersecurity measures, risk management, and incident reporting.

aws User Group Ljubljana

About NIS-2 Directive

1811 SOLUTIONS

- **The European Union** issued the upgraded **NIS 2 Directive (Network and Information Security Directive 2)** requiring **all EU member states (27)** to transpose it into their national legislation by **October 17, 2024.** However, several countries have **not yet completed this process**. Notably, **Belgium, Croatia, Hungary, Italy, Latvia, and Lithuania have successfully incorporated** it into their national laws and by design every law could be a little different (differences in enforcement, penalties, and specific requirements for compliance).

- In **Slovenia**, the NIS 2 directive will be implemented through the **Zakon o informacijski varnosti (ZInfV-1)**. This law is currently **in the final stages of inter-ministerial coordination**.

EVA 2023-1144-0005

OSNUTEK PREDLOGA

15. 5. 2024

II. BESEDILO ČLENOV

ZAKON
O INFORMACIJSKI VARNOSTI

I. Splošne določbe

1. člen
(vsebina zakona)

(1) Zakon ureja področja informacijske in kibernetske varnosti ter opredeljuje nacionalni sistem informacijske varnosti v Republiki Sloveniji. Pri tem ureja pristojnosti, naloge, organizacijo in delovanje pristojnega nacionalnega organa za informacijsko varnost (v nadaljnjem besedilu: pristojni nacionalni organ), organa za obvladovanje incidentov velikih razsežnosti in kriz, enotne kontaktne točke za kibernetsko varnost (v nadaljnjem besedilu: enotna kontaktna točka), skupine za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT), okvira sprejem Strategije kibernetske varnosti Republike Slovenije in določa kibernetsko obrambo ter sodelovanje pristojnih državnih organov in skupin CSIRT.

(2) Ta zakon članki nemotenega delovanja države v vseh varnostnih razmerah ter za ohranitev ključnih družbenih in gospodarskih dejavnosti v Republiki Sloveniji določa tudi ukrepe za obvladovanje tveganj za kibernetsko varnost in obveznost poročanja zavezancev po tem zakonu in prostovoljno prijavljenih incidentov. Uvaja tudi pravila in obveznosti glede izmenjave informacij o kibernetski varnosti ter nadzor po tem zakonu vključno za področje certificiranja kibernetske varnosti.

2. člen
(namen zakona)

(1) Namen zakona je sistemska ureditev področja informacijske ozirona kibernetske varnosti in zagotovitev visoke ravni kibernetske varnosti vključno s krepitvijo zaupanja v proizvode IKT, storitve IKT in postopke IKT ter njihove varnosti v Republiki Sloveniji na področjih, ki so bistvenega pomena za nemoteno delovanje države ter ohranitev zagotavljanja ključnih družbenih in gospodarskih dejavnosti v vseh varnostnih razmerah.

(2) S tem zakonom se v pravni red Republike Slovenije prenaša Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremenitvi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (Direktiva NIS 2) (UL L št. 333/142, z

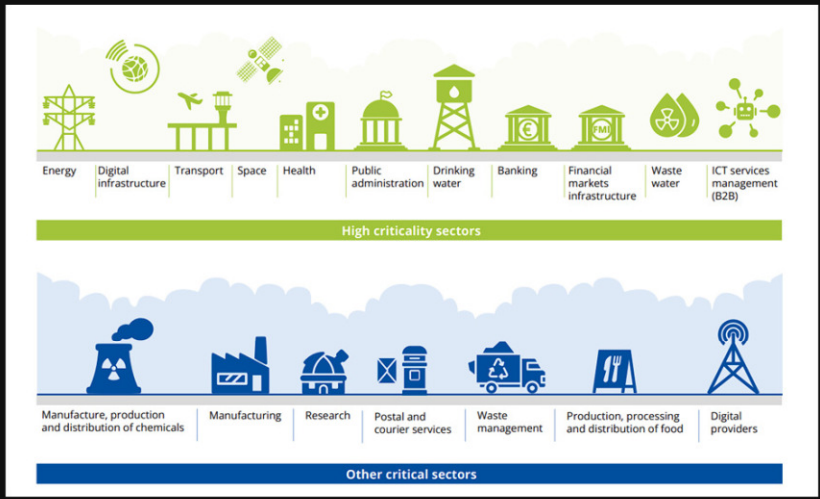
- When implementing the **NIS 2 Directive** |Zakon o informacijski varnosti (ZInfV) several other relevant regulations must be considered that impact cybersecurity and organizational operations in Slovenia / EU **(ZVOp-2, ZDR-1Cybersecurity Act (EU 2019/881), Cyber Resilience Act, Digital Operational Resilience Act (DORA),etc...).**

aws User Group Ljubljana

Sectors:

1811 SOLUTIONS

The NIS2 Directive defines several sectors essential for the functioning of the economy and society, categorizing them into **sectors of high criticality** and **other critical sectors**.



Pictures taken from infographic / source:
EU agency for Cybersecurity -
https://www.enisa.europa.eu/

■ 1	■ 2	■ 3	■ 4
All entities are required to implement risk management measures.	All entities are required to report significant cybersecurity incidents.	Essential entities are subject to ex ante & ex post supervision.	Important entities are subject to ex post supervision only.

The subjects are more precisely defined in **Article 6** and **Annexes I and II**.

6. člen
(zavezanci)

(1) Subjekti, ki spadajo v področje uporabe tega zakona po 3. členu tega zakona, so zavezanci po tem zakonu in se delijo na bistvene in pomembne subjekte.

(2) Za namene tega zakona se šteje, da so bistveni subjekti:
1.subjekti vrste iz Priloge I, ki imajo vsaj 250 zaposlenih in letni promet vsaj 50 milijonov evrov ali letno bilančno vsoto vsaj 43 milijonov evrov;
2. ponudniki kvalificiranih storitev zaupanja in registri vrhnjih domenskih imen ter ponudniki storitev DNS, ne glede na njihovo velikost;
3. ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, ki imajo vsaj 50 zaposlenih in letni promet oziroma letno bilančno vsoto vsaj 10 milijonov evrov;
4. subjekti javne uprave na državni ravni;
5. vsi drugi subjekti vrste iz Prilog I ali II, ki jih na podlagi 2. do 5. točke drugega odstavka 3. člena tega zakona in na predlog pristojnega nacionalnega organa določi vlada;
6. subjekti, ki so določeni kot kritični na podlagi zakona, ki ureja kritično infrastrukturo;
7. subjekti, ki so bili v skladu z Zakonom o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23) določeni kot izvajalci bistvenih storitev pred 16. januarjem 2023;
8. subjekti iz sektorja 9. Upravljanje storitev IKT Priloga I in niso subjekti iz točk 1 do 7 tega odstavka, ki jih na podlagi poimenskega seznama, ki ga pristojni organi po zakonu, ki ureja izvajanje Uredbe (EU) 2022/2554, posredujejo pristojnemu nacionalnemu organu, določi vlada.

(3) Za namene tega zakona se šteje, da so pomembni subjekti:
- subjekti vrste iz Prilog I ali II vključno s tistimi, ki jih na podlagi 2. do 5. točke drugega odstavka 3. člena tega zakona in na predlog pristojnega nacionalnega organa določi vlada z odločbo in
- drugi subjekti oziroma organi iz 3. člena tega zakona,

ki se ne štejejo za bistvene subjekte na podlagi prejšnjega odstavka.

(4) Ne glede na določbo 7. točke drugega odstavka tega člena Banka Slovenije ni zavezanec po tem zakonu.

(5) Določbe prvega, drugega in tretjega odstavka tega člena ne veljajo za druge fizične in pravne osebe iz dvanajstega odstavka 3. člena tega zakona, ki se za njih uporablja v delu, ki ureja certifikacijski okvir za kibernetsko varnost.

Text / Pictures taken from document - legislation: Zakon o Informacijski varnosti – osnutek predloga verzija 15.5.2024.

aws User Group Ljubljana

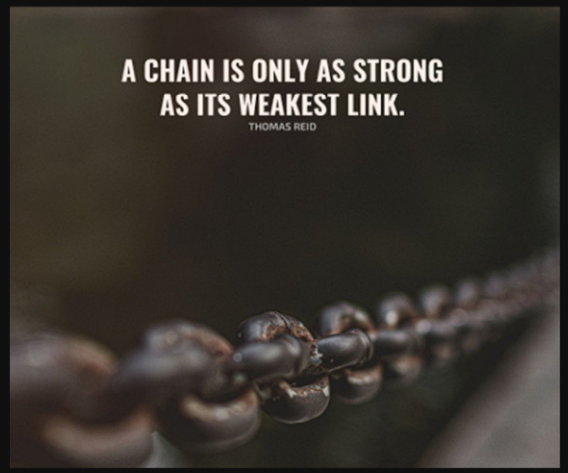
Purpose of directive:

1811 SOLUTIONS

The purpose of the directive is to enhance **cybersecurity resilience**, improve **incident response** and **risk management**, and ensure the continuity of **essential services**, while promoting trust and supporting **digital transformation** across critical sectors.

This is achived by:

- **Build and enhance Cybersecurity resilience of every interconnected entity.**
- **Strengthen Collective Defense of EU in all member states and their suppliers.**
- **Ensure Essential and Important Services Continuity.**
- **Shared Threat Intelligence.**
- **Zero Trust Architecture. Cyber Hygiene Practice.**
- **Implement Robust Cyber Risk Management.**
- **Mandatory Incident Reporting.**
- **Regular Security Audits and Risk Assessments**
- **Supply Chain Security.**
- **Promote Trust in Digital Systems. Data Encryption in transit and rest.**
- **Adherence to Regulatory Standards.**
- **Support Digital Transformation.**
- **Continuous Improvement.**



aws User Group Ljubljana

Important details:

1811 SOLUTIONS

Self-Registration:The national authority will establish a mechanism for **self-registration** within **two months** after the law is adopted.Entities subject to the law must **identify themselves** and **register in the system and appoint responsible person**. They must also **report any changes in responsible persons** promptly. Re-check minimum every 2 years.

Complience: Compliance measures must be implemented within six months for entities previously defined under NIS1 and within one year for all other relevant entities in alignment with regulatory mandates. Periodics assesments and rechecks.

European and Slovenian Cybersecurity Centers: Cybersecurity Information connected HUB! Detected Important Incident must be submitted within 24 hours of recogniznition. Full incident report must be submitted within 72 hours, including details on severity, impact, and initial evaluations.
In Slovenia, the Office of the Government of the Republic of Slovenia for Information Security serves as the National Coordination Centre for cybersecurity. For reporting cybersecurity incidents, the **Slovenian Computer Emergency Response Team (SI-CERT)** is the designated national authority.

SIGOV-CERT: A specialized CSIRT division within the Government Information Security Office and threat alerts.

European Cybersecurity Competence Centre (ECCC): Enhances cybersecurity innovation, critical infrastructure, and EU-wide collaboration. Headquarters in Bucharest, Romania

Certification Requirements: ICT products, services, and processes used by regulated entities must comply with **EU cybersecurity certification schemes**, as outlined in **Regulation (EU) 2019/881 and Cybersecurity resilience act**.

aws User Group Ljubljana

1811 SOLUTIONS

Key Focus Areas for NIS-2 Compliance:

PEOPLE

Properly train all users and administrators / c-level personal to ensure they understand their roles and responsibilities in cybersecurity and compliance.

DOCUMENTATION

Maintain comprehensive policies, procedures, and records to demonstrate alignment with NIS-2 requirements.

IMPLEMENTATIONS

Deploy the necessary security measures, tools, and systems to meet regulatory standards effectively.

PROCESSES

Establish and refine operational workflows for incident response, risk management, disaster recovery, business continuity and continuous improvement ensuring uninterrupted operations. Plan and execute assessments and Cybersecurity audits.

REGULATORY OBLIGATIONS

aws User Group Ljubljana

1811 SOLUTIONS

Determine Involvement!

Assess if your organization is subject to NIS-2 requirements in any way.

Get Management Approval!

Secure support and resources for company compliance efforts.

Where to start?

Create a Project group!

Form a team to manage compliance and cybersecurity initiatives, give them **authority**, invest in their **training for them to gain required knowledge** to use frameworks or controls (NIST 800 – series (CSF, RMF, other) / ISO/IEC 27000 family/ CIS controls,etc.).

Create and execute a action plan!

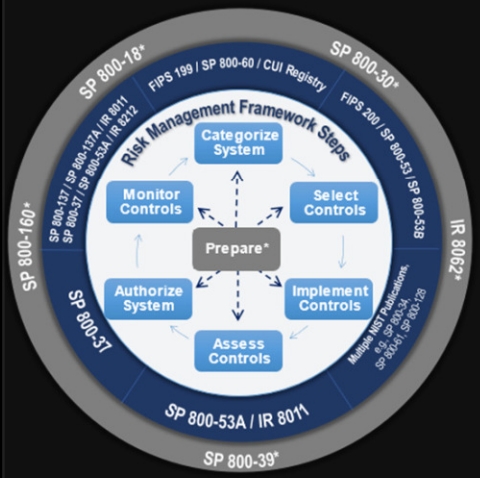
Develop a compliance plan with clearly defined deadlines, responsibilities, budget and measurable targets to ensure systematic progress and adherence to regulatory requirements.

aws User Group Ljubljana

“The action plan”

1811 SOLUTIONS

Establish a **baseline of the company's IT maturity level** by identifying **key organizational areas**, mapping **critical assets**, conducting a **Business Impact Analysis (BIA),** calculating **baseline and target maturity levels**, **analyzing and closing the gaps**, **determining risk tolerance**, and developing a comprehensive **risk management strategy**, including response and eradication plans, to align with industry frameworks and drive continuous improvement.



The **National Institute of Standards and Technology (NIST)** and the **International Organization for Standardization/International Electrotechnical Commission (ISO/IEC)** have developed frameworks that can help organizations achieve compliance with cybersecurity and information security standards.

ISO

aws User Group Ljubljana

People / Training

1811 SOLUTIONS

Train your NIS-2 project/implement/coordinator/managment team members.

Regular Security Awareness Training for all employees**.**

Specialized Training for IT Department Members (Administrators and Other Staff), HR, Legal, and C-Level Executives, including career development and certification paths, ensures that each group is equipped with the knowledge and skills required to address their specific roles in cybersecurity.

Criminal Record Checks for critical employees to ensure trustworthiness.

IT personal participation in Cybersecurity Defense Drills.

Role-playing and Testing Scenarios to validate Plans and Procedures (recovery, incident management, and operational plans).

Cross-training Personnel to cover roles during disasters or personnel shortages

Specific Skills Training in areas such as forensics and incident management

aws User Group Ljubljana

Documentation

1811 SOLUTIONS

Baseline/Core Security Documentation (Inventory, Technical documentation, Policies, Regulations, Forms, Standard Operating Procedures, and Plans).

Risk and Cyber-Risk Management Plan (validation of controls,regular assessments are mandatory).

Business Continuity Plan (BCP),supported by Business Impact Analysis(BIA) and performing periodic regular tests of it.

Disaster recovery plan and performing periodic regular tests of it.

Incident Management Plan, reporting capabilities and periodic test have to be in place and executed.

Communication plan and performing periodic regular tests of it.

Training and Exercise Records Documentation

Guidelines for Secure Information Exchange.

Cybersecurity Audits and assessments records.

Self-Assessment of Compliance (SAMOOCENE SKLADNOSTI) and yearly report!

Logs!

aws User Group Ljubljana

Implementations of Hardware and software to achieve cyber -hygiene

1811 SOLUTIONS

Main goal is to **minimize exposure to cyber threats** and reduce companies overall attack surface, by implementing:

- **Data and configuration Backup.**
- **Up-to-Date Hardware and Software.**
- **Only officially supported systems and appliances** (Windows 10 end of official support next year, etc.).
- **Vulnerability Management.**
- **Patch Management.**
- Endpoint Detection and Response (**EDR**), Extended Detection and Response (**XDR**), Managed Detection and Response (**MDR**), and Security Operations Center (**SOC**), **E-mail security**.
- Security Information and Event Management (**SIEM**) , Security Orchestration, Automation, and Response (**SOAR**).
- **Secure Network Architecture** (Implement next-generation firewalls, IDS/IPS, DDoS Protection, Switch Security,etc.).
- **Cryptography** (Encrypt sensitive information to prevent unauthorized access, encrypt data in transit and rest).
- **Multi-Factor Authentication** (MFA).
- **System Hardening** (STIGs - Security Technical Implementation Guides)
- **Advanced Cybersecurity Measures** (Zero Trust architectures, User Behavior Analytics (**UBA**), Privileged Access Management (**PAM**), and conduct manual or automatic, periodic testing of controls,etc.).
- Service Level Agreements (**SLA**) and **Redundancy** for Important Equipment.
- **EU cybersecurity certified products / services/ procedures**!

aws User Group Ljubljana

Process / Procedures

1811 SOLUTIONS

Processes and procedures link everything together by providing a structured approach that integrates periodic testing, centralized documentation, systematic assessment, and thorough auditing, ensuring continuous improvement and alignment with organizational goals and compliance standards.

- **Risk Management Processes:** Identify, assess, and mitigate cybersecurity risks with regular reviews.
- **Incident Management Procedures**: Detect, report, respond to, and analyze incidents to prevent recurrence.
- **Supply Chain Security Procedures:** Assess and monitor third-party risks; enforce cybersecurity requirements in contracts.
- **Business Continuity and Disaster Recovery Procedures:** Ensure service availability and test recovery plans for effective restoration.
- **Governance and Accountability Procedures:** Define roles, train staff, and ensure leadership accountability in cybersecurity.
- **Monitoring and Evaluation Procedures:** Gather threat intelligence, manage vulnerabilities, and track performance metrics.
- **Information Sharing and Cooperation:** Share threat intelligence and coordinate with national and EU authorities.
- **Compliance and Audit Procedures:** Conduct regular audits, maintain documentation, and ensure adherence to regulations.

aws User Group Ljubljana

REGULATORY OBLIGATIONS

1811 SOLUTIONS

Regulatory obligations outlined in the legislation emphasize the mandatory responsibilities of entities, including self-registration within specific timeframes, regular updates to provided data, and the maintenance of compliance with cybersecurity standards. Critical incidents and changes must be reported promptly, ensuring transparency and cooperation with national authorities and the EU.

Governance and Accountability: Assign clear responsibilities for cybersecurity within the organization and ensure that management bodies are accountable for implementing and overseeing cybersecurity measures.

Information Sharing and Cooperation: Participate in information-sharing networks to exchange cybersecurity threat intelligence. Cooperate with national and EU authorities to enhance collective cybersecurity resilience.

Compliance and Penalties: Adhere to the requirements set forth in the ZInfV and NIS2 Directive. Be aware that non-compliance can result in significant penalties, including fines and other corrective measures.

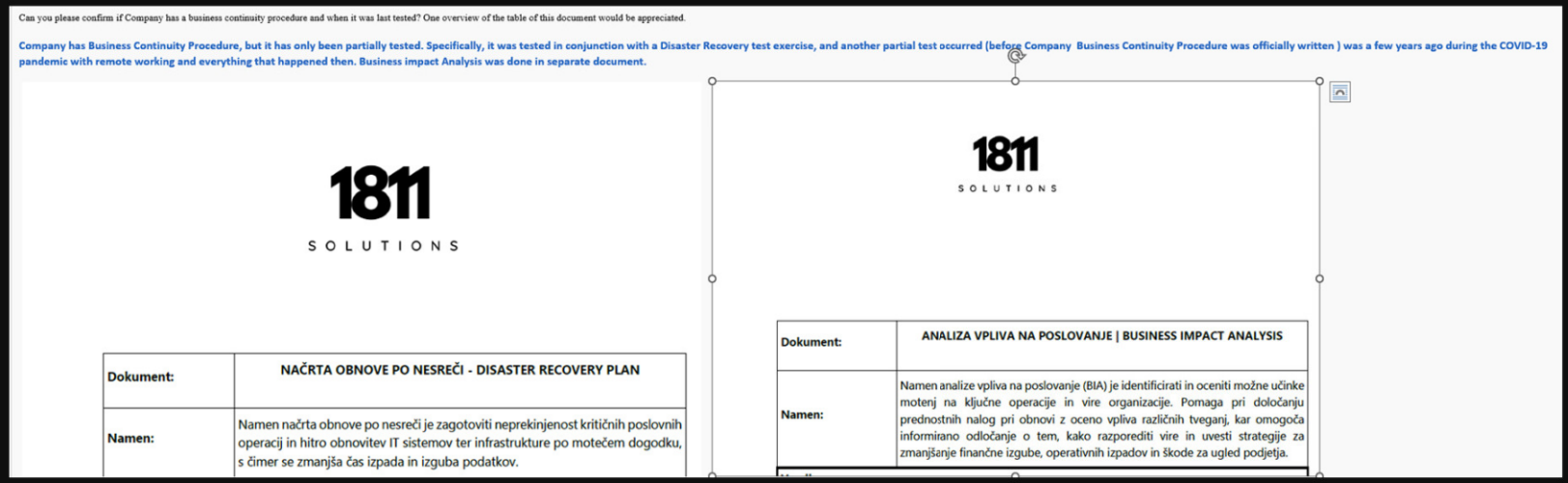
Organizations operating in Slovenia should familiarize themselves with the specific provisions of the ZInfV to ensure full compliance with national and EU cybersecurity regulations.

Being audited as supplier

What ever you do , just don’t give this kind of answer!

Je vaš datacenter ustrezno zaščiten? (Does your critical systems and assets reside in an isolated building managed by the organization or a third party that is controlled?).
Datacenter je postavljen po vseh varnostnih standardih

Answers should be as required, informative, truthful and closed ended!



Can you please confirm if Company has a business continuity procedure and when it was last tested? One overview of the table of this document would be appreciated.

Company has Business Continuity Procedure, but it has only been partially tested. Specifically, it was tested in conjunction with a Disaster Recovery test exercise, and another partial test occurred (before Company Business Continuity Procedure was officially written) was a few years ago during the COVID-19 pandemic with remote working and everything that happened then. Business impact Analysis was done in separate document.

1811 SOLUTIONS

Dokument:	NAČRTA OBNOVE PO NESREČI - DISASTER RECOVERY PLAN
Namen:	Namen načrta obnove po nesreči je zagotoviti neprekinjenost kritičnih poslovnih operacij in hitro obnovitev IT sistemov ter infrastrukture po motečem dogodku, s čimer se zmanjša čas izpada in izguba podatkov.

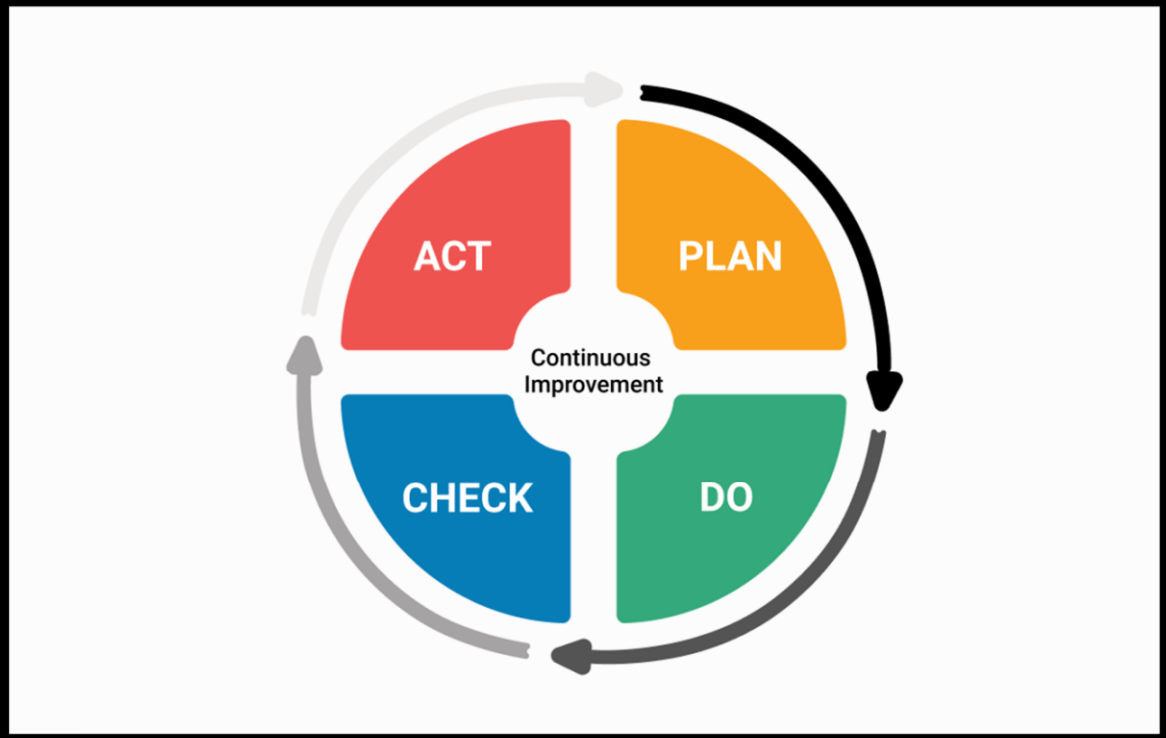
1811 SOLUTIONS

Dokument:	ANALIZA VPLIVA NA POSLOVANJE | BUSINESS IMPACT ANALYSIS
Namen:	Namen analize vpliva na poslovanje (BIA) je identificirati in oceniti možne učinke motenj na ključne operacije in vire organizacije. Pomaga pri določanju prednostnih nalog pri obnovi z oceno vpliva različnih tveganj, kar omogoča informirano odločanje o tem, kako razporediti vire in uvesti strategije za zmanjšanje finančne izgube, operativnih izpadov in škode za ugled podjetja.

aws User Group Ljubljana

FUTURE – What to keep in mind

1811 SOLUTIONS



aws User Group Ljubljana

1811 SOLUTIONS

Thank you!