ORDER

No. xxx/dd.mm.yyyy

for the approval of the criteria and thresholds for determining the degree of disruption of a service and the methodology for assessing the risk level of entities

Considering the provisions of art. 10 paragraph (2) and art. 18 of Government Emergency Ordinance no. 155/2024 on the establishment of a framework for the cybersecurity of networks and information systems in the national civil cyberspace, the provisions of art. 5 letter b) and art. 7 paragraph (3) - (4) of Government Emergency Ordinance no. 104/2021 on the establishment of the National Cyber Security Directorate, approved with amendments and completions by Law no. 11/2022, with subsequent amendments,

The Director of the National Cyber Security Directorate issues this Order:

Art. 1 – (1) Entities, as defined in art. 4 letter f) of Government Emergency Ordinance no. 155/2024 on the establishment of a framework for the cybersecurity of networks and information systems in the national civil cyberspace, which have not been qualified as essential entities or important entities according to art. 5 paragraph (1) letters a), c) - f), paragraph (2) - (4), art. 6 paragraph (1) and paragraph (2) letters b) and c) nor according to art. 9 letters a) and d) of the same normative act, shall assess the degree of disruption of services in order to complete the information requested according to the order of the director of the National Cyber Security Directorate for the approval of the requirements regarding the notification process for registration and the method of transmitting information.
(2) Disruption of a service, within the meaning of this order, means the interruption or impairment of the confidentiality or functioning of the respective service.
(3) When assessing the degree of disruption, entities shall refer to all the services they provide and which fall within Annexes No. 1 and 2 to Government Emergency Ordinance No. 155/2024.

Art. 2 – The results of the self-analysis regarding the fact that the entity is the sole provider of a service that is essential for supporting critical societal and economic activities, according to the provisions of art. 9 letter a) of Government Emergency Ordinance no. 155/2024, as they were transmitted in application of the order for the approval of the requirements regarding the notification process for registration and the method of transmitting information issued pursuant to the provisions of art. 18 of the same normative act, shall be interpreted in accordance with the provisions of art. 5 paragraph (1) letter b), respectively according to the provisions of art. 6 paragraph (2) letter a) of the
aforementioned normative act, as follows: a) an entity that is the sole provider in Romania of a service provided for in Annex no. 1 to Government Emergency Ordinance no. 155/2024 is an essential entity if it has not been identified as such according to the other criteria
provided for in art. 5 of the same normative act; b) an entity that is the sole provider in Romania of a service provided for in Annex no. 2 to Government Emergency Ordinance no. 155/2024 is a significant entity if it has not been identified as such according to the other criteria provided for in art. 6 of the same normative act.

Art. 3 – The criteria and thresholds for determining the degree of disruption of a service, provided in Annex no. 1 to this order, are approved.

Art. 4 – (1) The Methodology regarding the risk level assessment, provided for in Annex no. 2 to this order, is approved.

(2) The use of the methodology provided for in paragraph (1) aims to determine the category of technical, operational and organizational measures intended to identify, assess and manage risks related to the security of networks and information systems that the entity must implement.

(3) In order to determine the risk level of the entity, the National Cyber Security Directorate, in DNSC continues, establishes a base score for each sector in each annex to the Emergency Ordinance Government Decree No. 155/2024. The final score obtained by the entity determines the level of complexity of the measures security, related to the Cyber Fundamentals standard.

Art. 5 – (1) Entities calculate their score provided for in art. 3 using the calculation formulas provided for in the Annex no. 2, starting from the basic values related to the sector to which they belong, provided for in the annex to Methodology for assessing the risk level of entities, and in accordance with their size.

(2) An entity that carries out activities in several sectors shall assess its level of risk related to each sector and implement the level of security measures corresponding to the highest score obtained.

(3) When, following the assessment carried out by the entity, the values related to the impact and probability at the level of its own organization of the risks provided for in the methodology differ from the basic values of the sector on which the assessment is reported, the entity shall submit to DNSC an analysis containing a thorough justification for each value for which it requests a change in the basic value.

(4) Following the request provided for in paragraph (3), DNSC may validate the proposals submitted by the entity by the submitted request. In the event of their validation, the calculation of the score that determines the risk level of the entity is carried out according to the values thus updated.

Art. 6 – This order is published in the Official Gazette of Romania, Part I.

Director of the National Cyber Security Directorate
Dan - Petre CÎMPEAN

Annex No. 1

Criteria and thresholds for determining the degree of disruption of a service

Art. 1 – (1) The impact, as provided for in art. 9 of Government Emergency Ordinance no. 155/2024, is classified into:

a) high impact – when the disruption of the service has very serious and catastrophic consequences, at national level, on networks and information systems, assets, people, the state, the functioning of cross-sectoral services, or the functioning of cross-border services in the EU;

b) medium impact - when the disruption of the service has serious consequences, at national level, on networks and information systems, assets, people, the state, the functioning of cross-sectoral services, or the functioning of cross-border services in the EU;

c) low impact - when the disruption of the service has low consequences, at national level, on the networks and IT systems and assets of the entity, on individuals, the state, the functioning of cross-sectoral services, or the functioning of cross-border services in the EU. Low consequences refer to the impact on the ability of an entity to fulfil its mission or objectives to such an extent that it is able to fulfil its core functions, but significantly reduces the effectiveness of these functions.

(2) The level of impact, as provided for in paragraph (1), shall be determined taking into account the following:

a) fundamental rights and freedoms;

b) the national economy;

c) the health and life of people;

d) financial impact;

e) defense, public order and national security;

f) cross-sectoral or cross-border impact.

Art. 2 – (1) Entities shall analyze the effect that the interruption or impairment of the confidentiality or functioning of the services they offer may generate, at national level, on fundamental rights and freedoms, on the national economy, on the health and life of individuals, depending on the financial impact, as well as on defense, public order and national security, as well as depending on the cross-sectoral or cross-border impact in relation to other Member States of the European Union.

(2) In order to determine the impact generated by the disruption of the service provided by the entity in accordance with the provisions of art. 9 letter b) of Government Emergency Ordinance no. 155/2024, the level of impact is assessed in accordance with art. 10 paragraph (1) letters a) - d).

(3) In order to determine the impact generated by the disruption of the service provided by the entity according to art. 9 letter c) of Government Emergency Ordinance no. 155/2024, the level of impact is assessed in accordance with art. 10 paragraph (1) letter f).

(4) In order to determine whether an entity is considered essential in accordance with the provisions of art. 5 paragraph (1) letter b) of Government Emergency Ordinance no. 155/2024, respectively whether it is important in accordance with the provisions of art. 6 paragraph (2) letter a) of the same normative act, the criteria provided for in art. 9 letters b) and c) of the aforementioned normative act shall be applied, as appropriate, as follows:

a) any entity from the sectors in Annex no. 1 to Government Emergency Ordinance no. 155/2024 that has not been identified as an essential entity according to the other criteria provided for in art. 5 of the same normative act, but which reaches or exceeds the high threshold of impact generated by the disruption of the service provided, is an essential entity.

b) any entity from the sectors in Annexes no. 1 and 2 to Government Emergency Ordinance no. 155/2024 that has not been identified as an important entity according to the other criteria provided for in art. 6 of the same normative act or has not been identified as an essential entity according to letter a), but which reaches or exceeds the average threshold of the impact generated by the disruption of the service provided, is an important entity.

Art. 3 – (1) The impact on fundamental rights and freedoms is high when the personal data of more than 1,000,000 people are affected or access to essential public services is affected for at least 115,000 people.

(2) The impact on fundamental rights and freedoms is medium when the personal data of more than 200,000 persons are affected or access to essential public services is affected for at least 25,000 persons.

Art. 4 – (1) The impact on the national economy is high when losses of over 0.1% of Romania's GDP are caused, when at least 25% of the value of essential services in one of the sectors in Annexes no. 1 and 2 to Government Emergency Ordinance no. 155/2024 is affected, and damage is caused to critical infrastructure, as provided for by Government Emergency Ordinance no. 98/2010 on the identification, designation and protection of critical infrastructures, with subsequent amendments and supplements.

(2) The impact on the national economy is medium when the provision of essential services in one of the sectors in Annexes no. 1 and 2 to Government Emergency Ordinance no. 155/2024 is affected, when the functioning of critical infrastructure is affected, as provided for by Government Emergency Ordinance no. 98/2010 on the identification, designation and protection of critical infrastructures, with subsequent amendments and supplements.

Art. 5 – (1) The impact on the health and life of people is high when the death, chronic illness or disability of more than 50 people is caused or when traumatic injuries are caused or the health of more than 115,000 people is affected.

(2) The impact on the health and life of people is medium when traumatic injuries are caused or the health of people is affected.

Art. 6 – (1) The financial impact is high when the loss of at least 2,500 lei is caused to at least 115,000 people.

(2) The financial impact is medium when the loss of at least 2,500 lei is caused to at least 25,000 people.

Art. 7 – (1) The impact on defense, public order and national security is high when the state's capacity to ensure defense, public order and national security is affected, as well as generating the inability to perform its main functions, or when serious damage is generated to the state's reputation or citizens' trust in it.

(2) The impact on defense, public order and national security is medium when the state's ability to ensure activities in the field of defense, public order and national security is affected, with potentially serious consequences for the safety of individuals and private property.

Art. 8 – (1) The cross-sectoral or cross-border impact is high when at least two sectors and at least 20% of essential services in at least one sector are affected, or when Romania's obligations arising from international law and multilateral frameworks can no longer be fulfilled.

(2) The cross-sectoral or cross-border impact is medium when at least two sectors and at least 5% of essential services in at least one sector are affected, or when Romania's capacity to fulfil its obligations under international law and multilateral frameworks is affected.

Annex No. 2

Methodology for assessing the risk level of entities

Art. 1 - (1) In order to support essential entities and important entities, DNSC develops two mechanisms specific, respectively:

a) a tool for assessing the risk level of an entity – ENIRE@RO;

b) a platform for enrollment, information and cooperation – NIS2@RO.

(2) The mechanisms are intended for all essential and important entities registered in the Register of Entities, and are used to establish the risk level of the entity in accordance with art. 18 paragraph (6) of Government Emergency Ordinance no. 155/2024. (3) If the

NIS2@RO Platform is unavailable or a pre-assessment of the risk level of an entity is desired, the ENIRE@RO Tool is used, which is downloaded from the DNSC websites (dnsc.ro, platformanis2.ro) and used locally.

Art. 2 - (1) The mechanisms calculate the risk level of entities from the perspective of five typologies of actors divided into two groups, based on the knowledge and resources at their disposal, respectively:

a) those with common-level capabilities: terrorists, ideologically motivated activists, and hostile competitors. They have common/low knowledge and limited resources needed to successfully execute a cyberattack;

b) those with extensive capabilities: cybercriminals and state actors. They have the advanced knowledge and vast resources necessary to successfully execute a cyberattack.

(2) To calculate the level of risk represented by each category of actors, 5 categories of cyber attacks are taken into account, depending on the intended purpose and the way in which the threat manifests itself, namely:

a) sabotage/disruption of service provision;

b) theft of information/espionage;

c) attacks specific to cybercrime;

d) hacktivism/defacement, dos/ddos;

e) attacks that target or affect the image of the entity.

Art. 3 - (1) The data and information used in the two mechanisms are:

a) Data with predefined values at sector level that cannot be modified:

i. Sector assessed - represents the field of activity of the entity analyzed. If the entity operates in multiple sectors, the risk level will be calculated separately for each sector, with the cybersecurity measures being implemented according to the highest score obtained;

ii. Nature of the attack - represents the main way of carrying it out, having a value pre-established by the DNSC for each sector, as follows: "global" - value "1" - indiscriminate attacks that target as many devices, services or users as possible, without having a specific victim, and "targeted" - value "2" - deliberate attacks on a specific entity, carried out by actors with sufficient expertise and resources, requiring a higher degree of protection.

b) Data to be modified according to the size of the entity. In accordance with the provisions of art. 8 of Government Emergency Ordinance no. 155/2024, taking into account the provisions of Law no. 346/2004 on stimulating the establishment and development of small and medium-sized enterprises, as subsequently amended and supplemented, an entity may be classified into:

i. large enterprise (L), in which case this parameter will have the value "3";

ii. medium-sized enterprise (M), in which case this parameter will have the value "2";

iii. small enterprise and micro enterprise (S), in which case this parameter will have the value "1".

In the case of public administration entities, the parameter will be calculated based on the average number of employees, calculated according to the provisions of art. 5 of Law 346/2004, as follows: up to 49 employees, it will have the value "1", between 50 and 249 employees, it will have the value "2", minimum 250 employees, it will have the value "3".

c) Data with predefined values at sector level and which can be modified, in a justified manner, by the entity:

i. Impact - represents the damage that may occur as a result of a cyber attack in the categories provided for in the provisions of art. 2 paragraph (2), carried out by a type of actor provided for in the provisions of art. 2 paragraph (1) and is determined in accordance with the criteria and thresholds for determining the degree of disruption of a service, provided for in Annex no. 1. The classification in the impact thresholds is reported to the attack category and the type of attacker. This variable may have the following levels: "high" - value "10", "medium" - value "5" or "low" - value "0";

ii. Probability - represents the chance that a risk of a cyber attack from the categories provided for in the provisions of art. 2 paragraph (2), carried out by a type of actor provided for in the provisions of art. 2 paragraph (1), will materialize, being a measure of the possibility of its occurrence, determined either by qualitative assessment or by quantification, depending on the nature of the risk and the available data. It can have the following levels: "high" - value "1" - the actor is known for similar attacks in the respective sector, and the risk is unacceptable, requiring immediate reduction measures or interruption of activity; "medium" - value "0.5" - the actor has carried out similar attacks globally, and the risk is tolerable, requiring monitoring and improvement actions in the medium and long term; "low" -
value "0" – there is no evidence that the actor has carried out such attacks in the sector, and the risk is acceptable without additional interventions.

d) Automatically calculated data:

i) The value of the risk;

ii) The entity's risk score.

(2) For each type of threat actor, the risk value is calculated according to each category of cyber attack.

(3) The value of the risk is determined by multiplying the following parameters: the size of the entity, as determined in the provisions of paragraph (1) letter b), the nature of the attack, as determined in the provisions of paragraph (1) letter a) point ii, the impact, as determined in the provisions of paragraph (1) letter c) point i and the probability, as determined in the provisions of paragraph (2) letter c) point ii).

The values obtained for a threat actor type, correlated with each attack category, are added together to determine the overall risk associated with that threat actor.

(4) The entity risk score is determined by adding the risk value associated with each threat actor type with each attack category and is equal to the sum of the overall risk values for all five threat actor types.

(5) The entity's overall score will determine its risk level, based on which the applicable cybersecurity requirement category is established, as follows:

a) entities that obtained a score between "0" and "99" points will implement the "Basic" level;

b) entities that obtained a score between "100" and "199" points will implement the "Important" level;

c) entities that obtained a score between "200" and "1,500" points will implement the "Essential" level.

(6) In order to apply the methodology, the entity registered in the Register of Entities uses exclusively one of the two mechanisms made available by the DNSC.

Art. 4 – (1) If an entity has not used the NIS2@RO Platform in the risk assessment process due to its unavailability, the entity will be obliged to complete and upload the report and supporting documents, as appropriate, within a maximum period of 20 days from the date on which it becomes available. The validation and confirmation of these actions will be carried out by the DNSC.

(2) DNSC recommends that all entities to which the provisions of Government Emergency Ordinance No. 155/2024 do not apply to implement the requirements of the Cyber Fundamentals standard, "Basic" level.

Art. 5 – The sectoral values for establishing the risk level, provided in the annex to this annex, are approved.

Art. 6 – (1) Entities in Sector 3. Banking sector and entities in Sector 9. Management of ICT services (business-to-business) in Annex no. 1 to Government Emergency Ordinance no. 155/2024 do not carry out the assessment of the risk level of the entity.

(2) The entities in Sector 3. Banking sector in Annex no. 1 to Government Emergency Ordinance no. 155/2024 referred to in paragraph (1) shall apply the risk management measures in terms of cybersecurity as provided for in *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.*

(3) The entities in Sector 9. Management of ICT services (business-to-business) from Annex no. 1 to Government Emergency Ordinance no. 155/2024 mentioned in para. (1) applies the cybersecurity risk management measures provided for in *Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down detailed rules for the implementation of Directive (EU) 2022/2555 as regards technical and methodological requirements for cybersecurity risk management measures and further specifying the cases in which an incident is considered significant in relation to DNS service providers, TLD registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online marketplaces, online search engines and social networking service platforms, and trust service providers.*

(4) Entities in Sector 4. Financial market infrastructures in Annex no. 1 to Government Emergency Ordinance no. 155/2024 to which *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience of the financial sector and amending Regulations (EC) no. 1060/2009, (EU) no. 648/2012, (EU) no. 600/2014, (EU) no. 909/2014 and (EU) 2016/1011 applies,* as well as entities in Sector 8. Digital infrastructure in Annex no. 1 to Government Emergency Ordinance no. 155/2024 to which *Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the implementation of Directive (EU) 2022/2555 as regards technical and methodological requirements for cybersecurity risk management measures and further specifying the cases in which an incident is considered significant with regard to*

DNS service providers, TLD name registries, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, online marketplaces, online search engines and social networking service platforms, as well as trust service providers, do not perform an assessment of the entity's risk level.

Sectoral values for determining the risk level

Risk \ Section		Energy		Transport		Financial		Health		Drinking water		Wastewater		Digital infrastructure		Public administration		Space		Food production, processing, distribution		Waste management		Manufacture of chemicals		Production, processing, distribution of food		manufacture		Providers		Research	
Attack category		overall	targeted	overall	targeted	overall	targeted	overall	targeted	overall	targeted	overall	targeted	overall	targeted	overall	targeted	overall	targeted	overall	targeted	overall	targeted	overall	targeted	overall	targeted	overall	targeted	overall	targeted	overall	targeted
terrorists - sabotage/disruption of service provision	Impact		R		R		R		R		R		R		R		R		R		R		M		R		R		M		R		M
	Probability		M		M		M		M		R		R		M		M		M		M		M		M		M		S		M		S
terrorists - information theft/espionage	Impact		R		R		R		R		M		M		R		R		R		M		S		M		S		R		M		R
	Probability		S		S		M		M		M		M		S		M		S		S		M		M		S		S		S		M
terrorists - cybercrime-specific attacks	Impact	R		R		R		R		M		M		R		R		R		R		M		R		R		S		M		R	
	Probability	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S	
terrorists - hacktivism/defacement, dos/ ddos	Impact M			M		M		S		S		S		M		R		M		S		M		M		M		S		S		M	
	Probability	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S	
terrorists - attacks that target or affect the image of the entity	Impact	S		S		S		M		S		S		S		R		M		S		S		S		M		S		M		S	
	Probability	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S	
ideologically motivated activists - sabotage/disruption of service provision	Impact		R		R		R		R		R		R		R		R		R		R		M		R		R		M		R		M
	Probability		S		S		M		M		M		M		M		M		S		M		S		S		S		S		M		S
ideologically motivated activists - information theft/espionage	Impact		R		R		R		R		M		M		R		R		R		M		S		M		S		R		M		R
	Probability		S		S		S		S		S		S		S		S		S		S		M		M		S		S		M		S
ideologically motivated activists - cybercrime-specific attacks	Impact	R		R		R		R		M		M		R		R		R		R		M		R		R		S		M		R	
	Probability	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S	
ideologically motivated activists - hacktivism/defacement, dos/ ddos	Impact M			M		M		S		S		S		M		R		M		S		M		M		M		S		S		M	
	Probability	M		M		M		S		s		S		M		M		M		S		S		S		M		M		S		M	
	Impact	S		S		S		M		S		S		S		R		M		S		S		S		M		S		M		S	

Risk \ Section		Energy		Transport		Industrial		Health		Drinking		Wastewater		Digital Infrastructure		Public Administration		Space-		Electronics		Warehousing		Production, processing, chemicals		Processing, Distribution		manufacture		Providers		Research	
ideologically motivated activists - attacks that target or affect the image of the entity	The probability is	M		M		M		M		S		S		M		M		M		M		M		M		M		S		M		S	
hostile competitors - sabotage/disruption of service provision	Impact		R		R		R		R		R		R		R		R		R		R		M		R		R		M		R		M	
	The probability is		S		S		S		S		S		S		S		S		S		S		S		S		S		M		S		S	
hostile competitors - information theft/espionage	Impact		R		R		R		R		M		M		R		R		R		M		S		M		S		R		M		R	
	The probability is		S		S		S		S		S		S		S		S		S		S		S		S		S		R		S		M	
hostile competitors - cybercrime-specific attacks	Impact	R		R		R		R		M		M		R		R		R		R		M		R		R		S		M		R		
	Probability	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		
hostile competitors - hacktivism/defacement, dos/ddos	Impact M			M		M		S		S		S		M		R		M		S		M		M		M		S		S		M		
	The probability is	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		
hostile competitors - attacks that target or affect the entity's image	Impact	S		S		S		M		S		S		S		R		M		S		S		S		M		S		M		S		
	Probability	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		
cybercriminals - sabotage/disruption of service provision	Impact		R		R		R		R		R		R		R		R		R		R		M		R		R		M		R		M	
	The probability is		M		S		S		S		S		S		S		M		S		M		S		S		S		S		S		S	
cyber criminals - information theft/espionage	Impact		R		R		R		R		M		M		R		R		R		M		S		M		S		R		M		R	
	The probability is		R		R		R		M		M		M		R		R		R		S		M		M		S		M		M		M	
cybercriminals - cybercrime-specific attacks	Impact	R		R		R		R		M		M		R		R		R		R		M		R		R		S		M		R		
	The probability is	R		R		R		R		M		M		R		R		R		R		R		R		M		R		R		R		
cybercriminals - hacktivism/defacement, dos/ddos	Impact M			M		M		S		S		S		M		R		M		S		M		M		M		S		S		M		
	The probability is	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		
cybercriminals - attacks that target or affect the image of the entity	Impact	S		S		S		M		S		S		S		R		M		S		S		S		M		S		M		S		
	The probability is	S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		S		
state actors - sabotage/disruption of service provision	Impact		R		R		R		R		R		R		R		R		R		R		M		R		R		M		R		M	
	The probability is		R		R		M		M		R		R		R		R		R		M		M		R		R		M		M		S	

Risk / Section		Energy		Transport		Finance		Health		Ordering		Wastewater		Digital Infrastructure		Public Administration		Space-		Electronics		Waste management		Production, processing, chemicals		Production, processing, distribution		manufacture		Digital providers		Research	
state actors - information theft/espionage	Impact		R		R		R		R		M		M		R		R		R		M		S		M		S		R		M		R
	Probability yourself		R		R		M		M		M		M		R		R		R		M		M		M		M		M		M		R
state actors - cybercrime-specific attacks	Impact	R		R		R		R		M		M		R		R		R		R		M		R		R		S		M		R	
	Probability yourself	S		S		S		S		S		S		S		S		S		S		S		S		S		M		S		S	
state actors - hacktivism/defacement, dos/ ddos	Impact M			M		M		S		S		S		M		R		M		S		M		M		M		S		S		M	
	Probability yourself	M		M		M		S		S		S		M		M		M		S		S		S		M		S		S		S	
state actors - attacks that target or affect the image of the entity	Impact	S		S		S		M		S		S		S		R		M		S		S		S		M		S		M		S	
	Probability yourself	S		S		S		S		S		S		S		S		S		S		S		S		S		S		M		M	
Standard score entity	small/micro	95		85		85		72,5		67,5		67,5		95		125		87,5		55		15		60		42,5		57,5		55		62,5	
	MEDIUM	190		170		170		145		135		135		190		250		175		110		30		120		85		115		110		125	
	great	285		255		255		217,5		202,5		202,5		285		375		262,5		165		45		180		127,5		172,5		165		187,5	

Legend:

Impact and probability can have the following values, noted in this table, as follows:

- Low - S
- Medium - M
- High - R