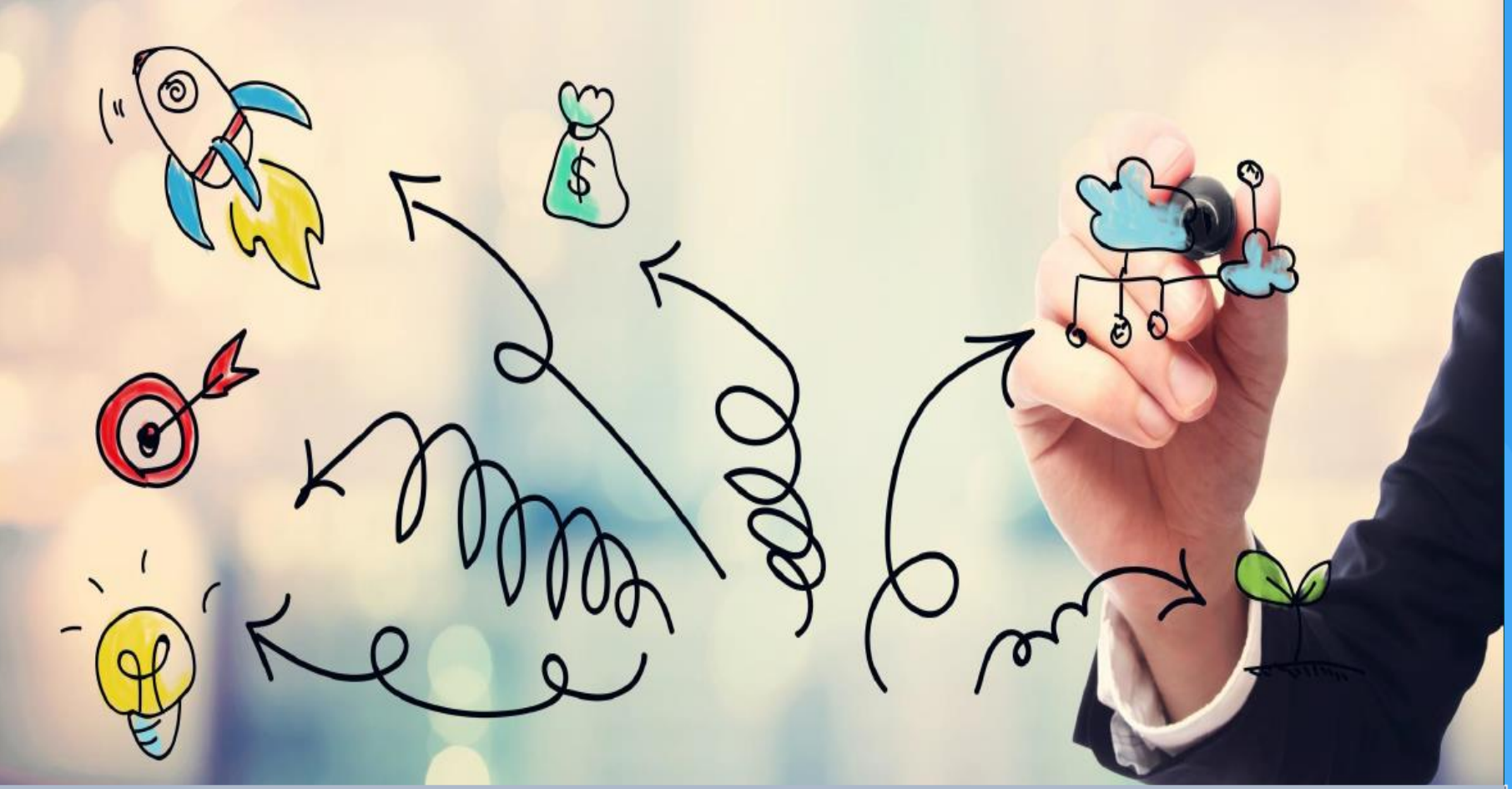


RISK CULTURE LAB

# Копроративно управление на киберсигурността

**Светлозар Каранешев, Risk Culture Lab**

22 април, 2020

София

SoftUni

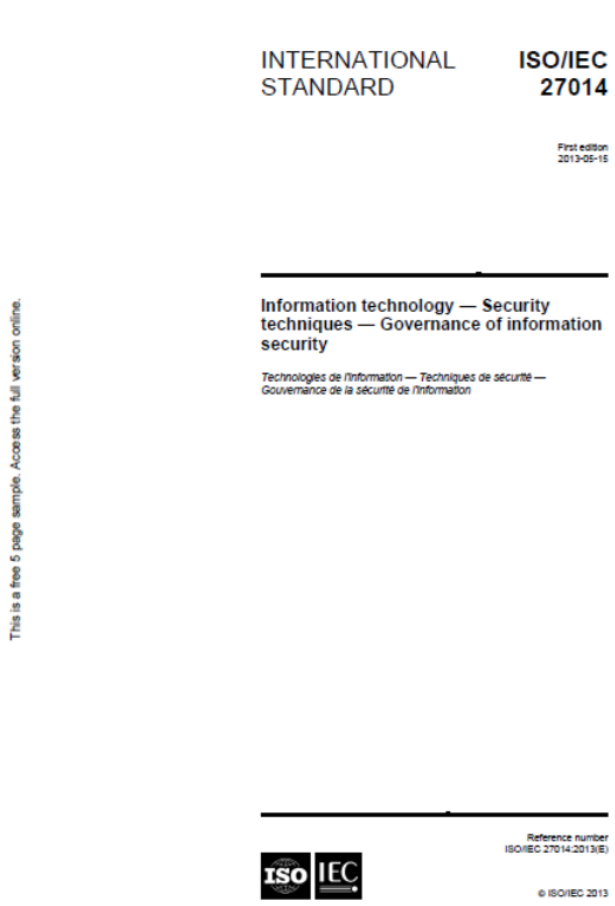
# Какво представлява киберсигурността?

RISK CULTURE LAB


<u>Киберсигурност:</u>

Защитата на информационните активи чрез справяне със заплахи за информация, обработвана, съхранявана и транспортирана от информационни системи, работещи в интернет.

# Рамка за корпоративно управление на киберсигурността




# ИСО/ИЕК 27014 – корпоративно управление на информационната сигурност


INTERNATIONAL STANDARD

**ISO/IEC 27014**

First edition
2013-05-15

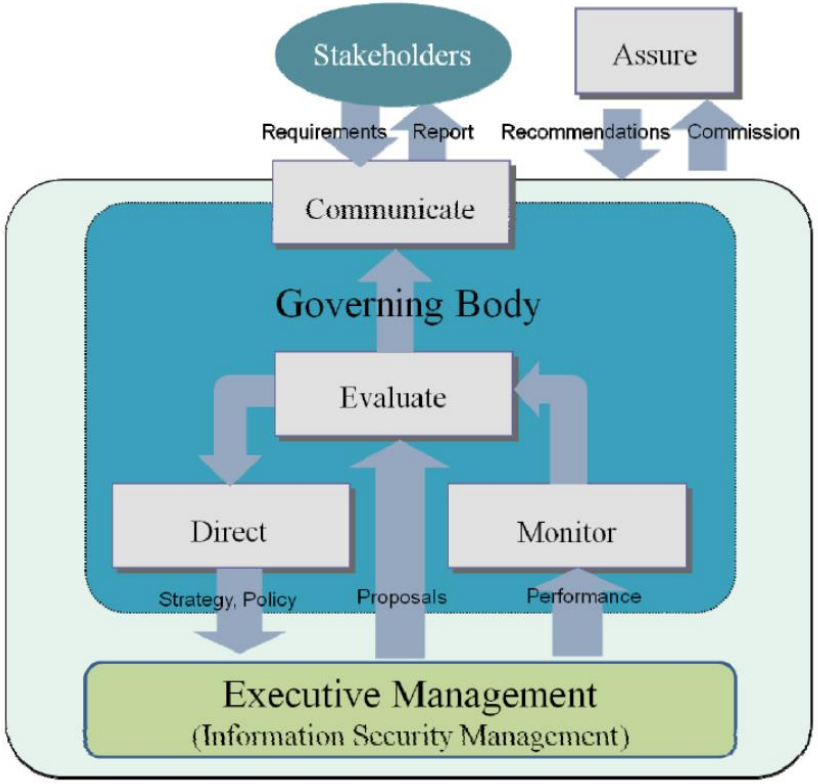
**Information technology — Security techniques — Governance of information security**

*Technologies de l'information — Techniques de sécurité — Gouvernance de la sécurité de l'information*

Reference number
ISO/IEC 27014:2013(E)

© ISO/IEC 2013





# ИСО/ИЕК 27014 – Приниципи на корпоративно управление на информационната сигурност

RISK CULTURE LAB

- Изграждане на информационна сигурност, която **обхваща цялата организация** – всички звена в организацията участват в управлението на информационната сигурност;
- **Прилага рисково базиран подход**, който е част от системата за управление на риска на организацията;
- **Определя инвестиционните решения** – разработва инвестиционна стратегия за информационна сигурност;
- Осигурява съответствие с вътрешни и външни изисквания;
- Насърчава позитивна среда и култура на сигурност;
- **Оценява качеството на информационна сигурност** в съответствие с организационните резултати.

SoftUni

# Корпоративно управление и киберсигурност

RISK CULTURE LAB


FERMA

Federation of European Risk Management Associations

FERMA обединява 21 асоциации за управление на риска в 20 европейски държави. Те представляват близо 5000 професионални мениджъри на риска, активни в широк спектър от бизнес сектори. FERMA действа от тяхно име на европейско ниво и насърчава професията за управление на риска.

ECIIA

EUROPEAN CONFEDERATION OF INSTITUTES OF INTERNAL AUDITING

Ролята на ECIIA е да подобри корпоративното управление чрез насърчаване на професионалната практика на вътрешен одит. Членове са 34 национални института за вътрешен одит от страни, представляващи 47 000 членове.

SoftUni

# Корпоративно управление и киберсигурност

RISK CULTURE LAB

Основа за разработването на рамката за корпоративно управление на киберсигирността са:

Препоръки на ОИСР за управление на цифоровите рискове за икономически и социален просперитет от 2015 година.

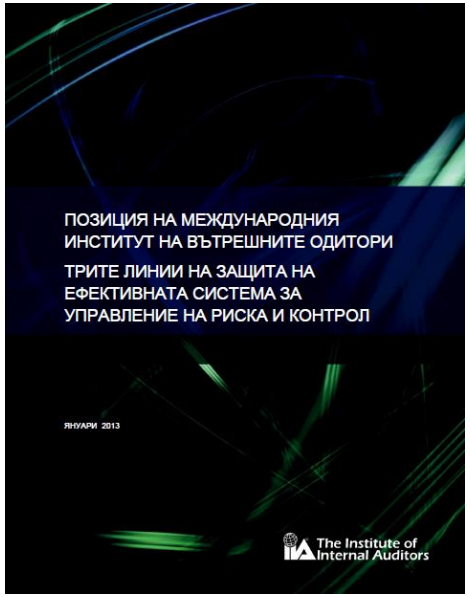
Моделът на трите линии на защита, предложен съвместно от FERMA и ECIIA през 2014 година.

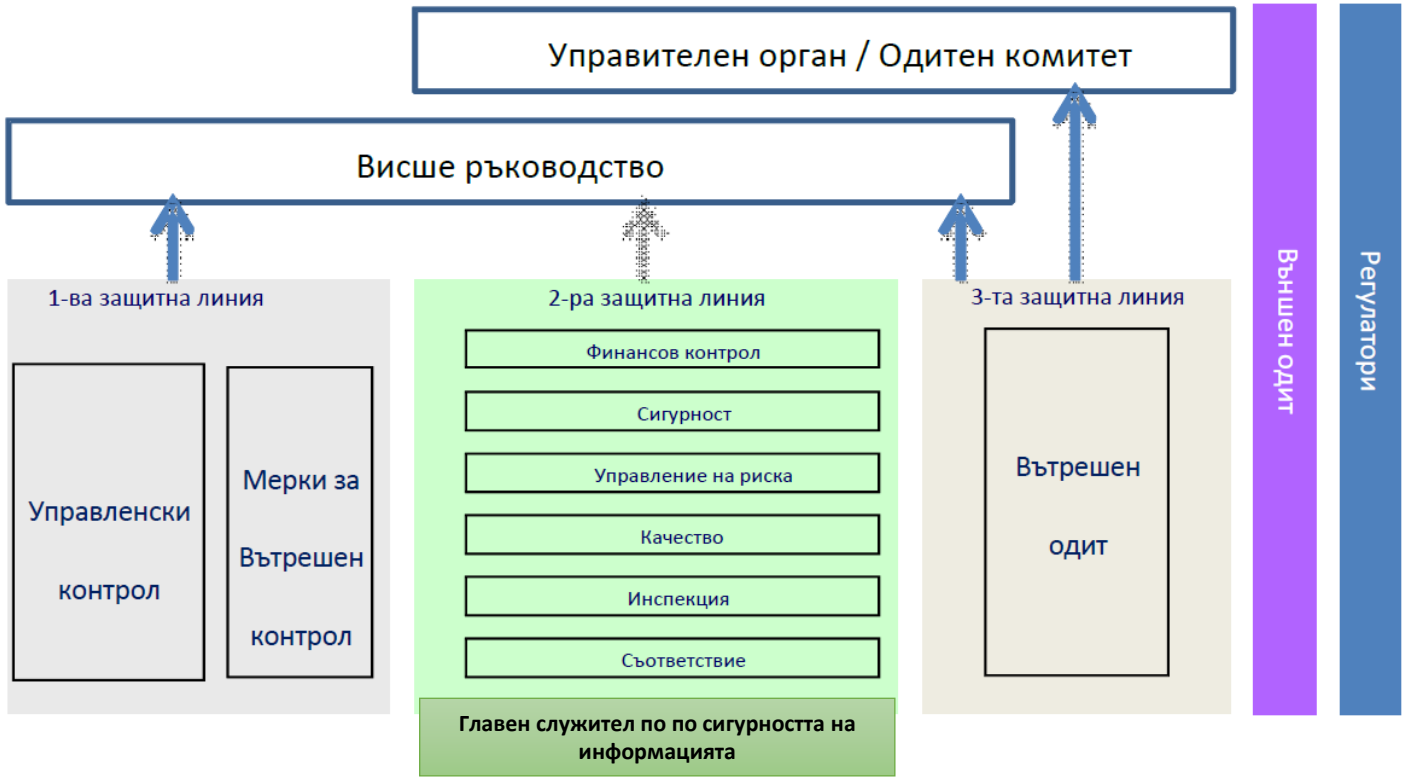
# Принципи на ОИСР за управление на цифоровите рискове

RISK CULTURE LAB

- Отговорност – висшето ръководство е отговорно за определяне на отговорностите при управлението на киберрисковете;
- Осведоменост, умения и овластяване – успешната програма за киберсигурност изисква пълен ангажимент на ръководството и всички служители;
- Оценка на риска – наличието на система за управление на риска е критично;
- Спазване на приложими закони и регулации;
- Кооперация базирана на добри комуникации и доверие в организацията;
- Показатели за сигурност – трябва да са избрани на основата на анализа на риска
- Иновации – иновациите подпомагат добрата киберсигурност;
- Подготвеност и приемственост – възможността от инциденти не може да се избегне напълно и за целта организациите трябва да разработват планове за такива ситуации.

# Моделът на трите линии на защита



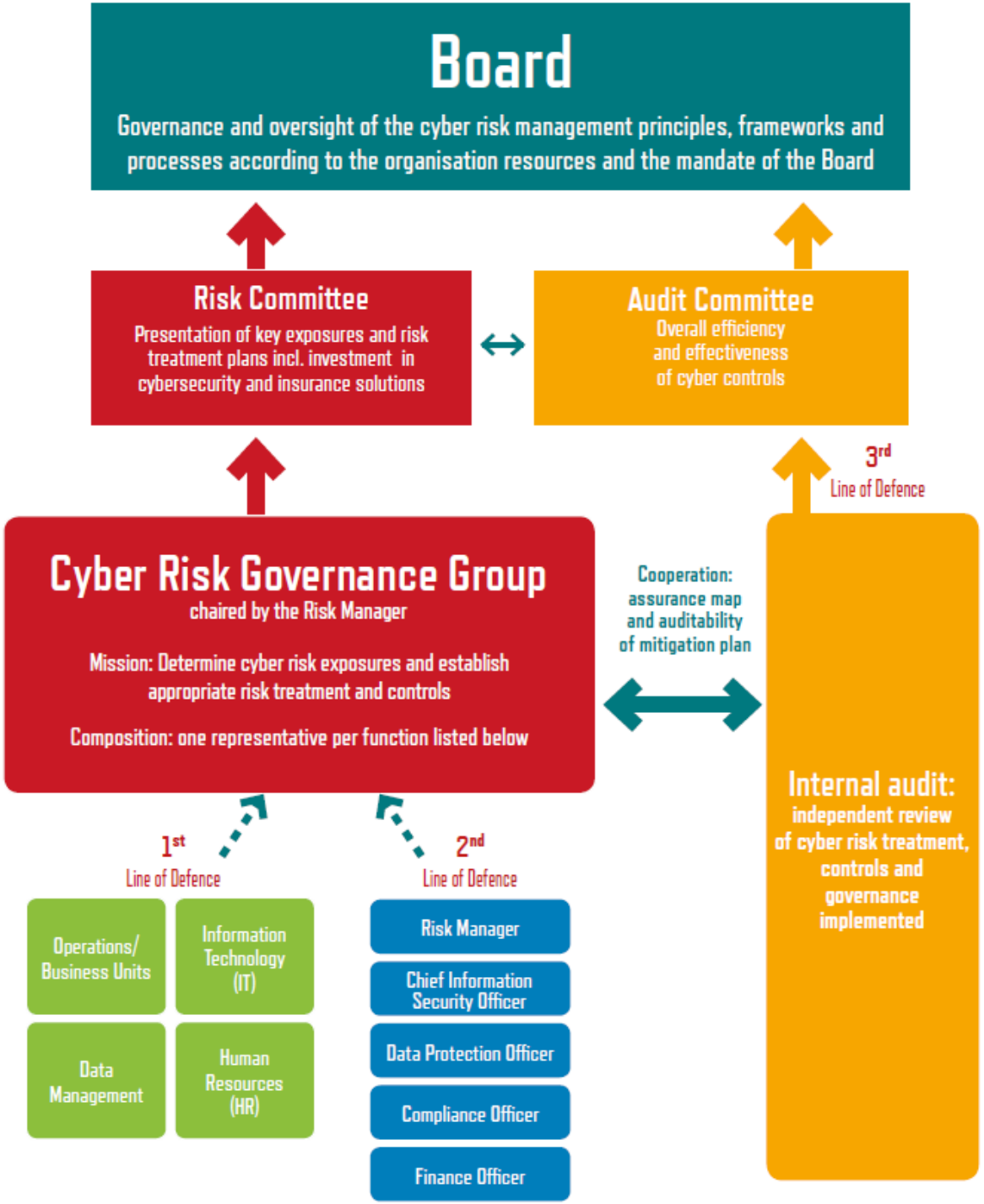




Моделът трите линии на защита разграничава три групи (или линии), участващи в ефективното управление на риска:

- Функции, които са собственици на рискове и ги управляват;
- Функции, които наблюдават рисковете;
- Функции, които осигуряват независима увереност.

Като първа линия на защита оперативните мениджъри са собственици нарисковете и ги управляват. Те също са отговорни за прилагането на коригиращи действия за справяне с недостатъците в процеса и контрол.

# Линии на защита и комитети



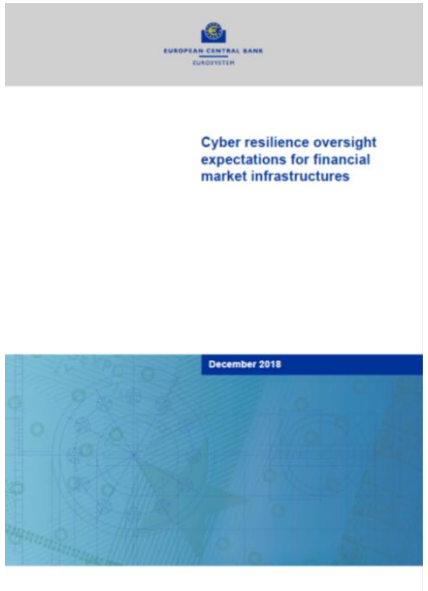

# Стратегия и програма за управление на киберсигурността

RISK CULTURE LAB

- **Стратегията за киберсигурност** определя целите за киберсигурност; изискванията към хора, процеси и технологии за управление на киберрисковете и изискванията към осъществяването на навременна комуникация между заинтересованите страни с цел ефективна реакция и възстановяване от кибер атаки.
- **Програмата за управление на киберсигурността** обхваща всички дейности и ресурси на организацията, които осигуряват услуги за киберсигурността на организацията.

SoftUni

# Рамка за корпоративно управление на киберсигурността и култура


Мениджмънтът промотира позитивна култура на информационна сигурност.

Управителният съвет и висшето ръководство трябва да популяризират култура, която признава, че служителите на всички нива имат важни отговорности за осигуряване на кибер устойчивост и да водят чрез пример.

# Полезни връзки

RISK CULTURE LAB


Предизвикателства пред ефективното прилагане на политиката за киберсигурност на ЕС

https://www.eca.europa.eu/bg/Pages/DocItem.aspx?did=49416

ISACA cybersecurity definition

https://www.isaca.org/resources/glossary

COBIT 2019 Framework: Introduction and Methodology,

https://www.isaca.org/bookstore/bookstore-cobit_19-digital/wcb19fim

ISO/IEC 27014:2013, Information technology — Security techniques — Governance of information security,

https://www.iso.org/standard/43754.html

At the junction of corporate governance and cybersecurity,

https://www.eciia.eu/wp-content/uploads/2019/02/FERMA-Perspectives-Cyber-risk-governance-09.10.2018_0.pdf

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security,
http://www.oecd.org/internet/ieconomy/15582260.pdf

ТРИТЕ ЛИНИИ НА ЗАЩИТА НА. ЕФЕКТИВНАТА СИСТЕМА ЗА. УПРАВЛЕНИЕ НА РИСКА И КОНТРОЛ,

https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control%20Bulgarian.pdf

Cyber resilience oversight expectations for financial market infrastructures,

https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

RISK CULTURE LAB

# Управление на киберрисковете

**Светлозар Каранешев, Risk Culture Lab**

22 април, 2020

София

SoftUni

RISK CULTURE LAB

"There are only two types of companies:
those that have been hacked,
and those that will be."

Robert Mueller
FBI Director, 2012

# ИКТ рисковете в топ 10 глобални рискове за 2019 и 2020 г

RISK CULTURE LAB

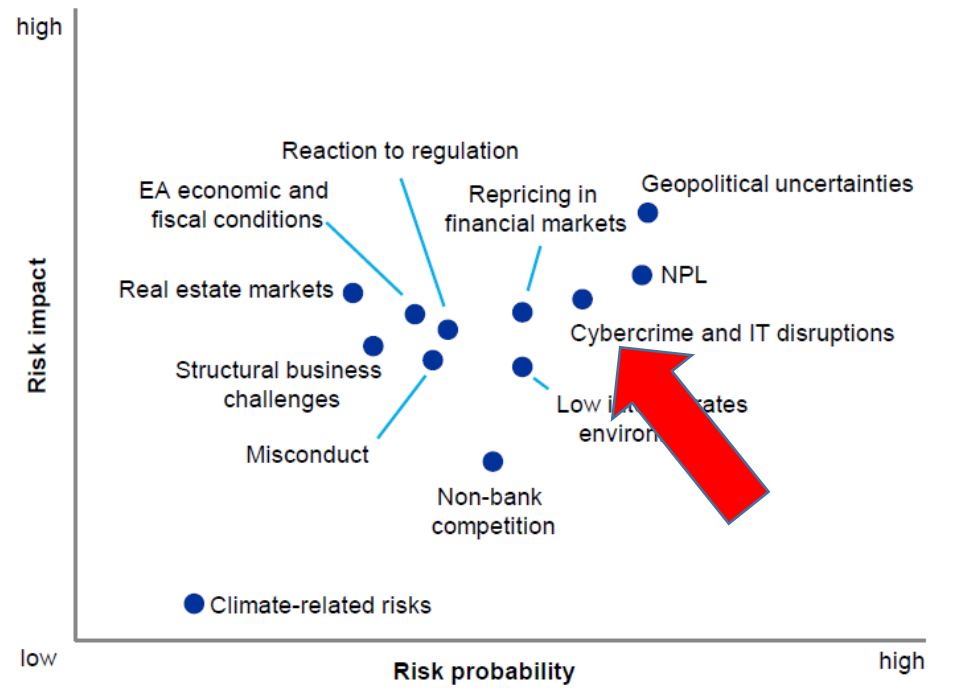
2019


2020

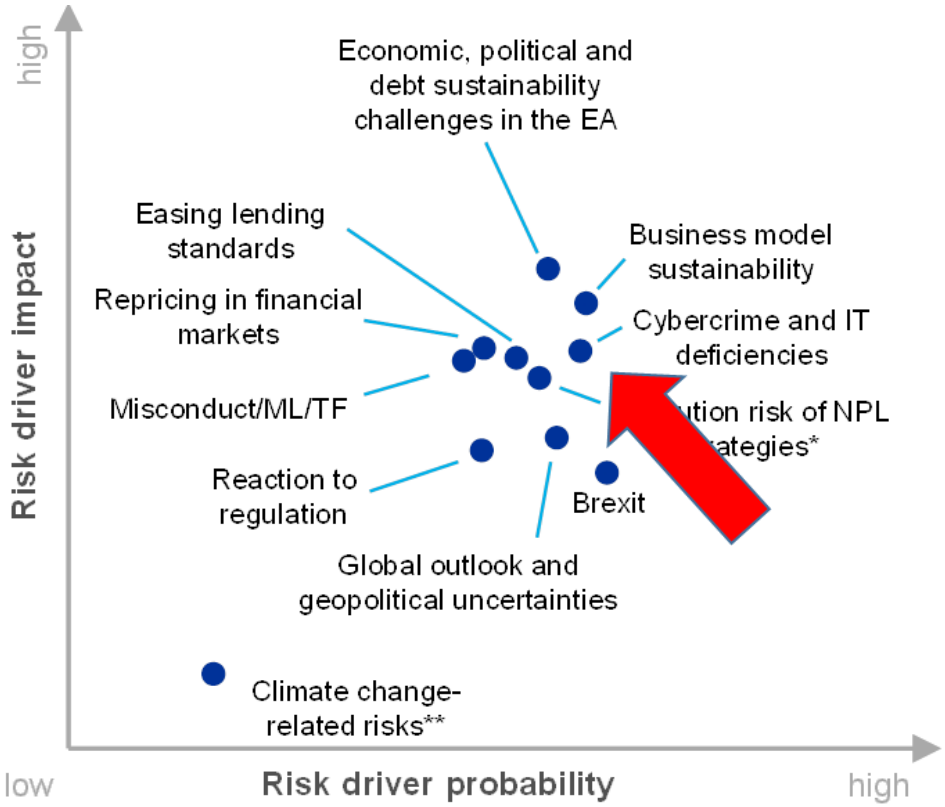

SoftUni

# Банков надзор на ЕЦБ: Оценка на риска за 2019 и 2020 г.

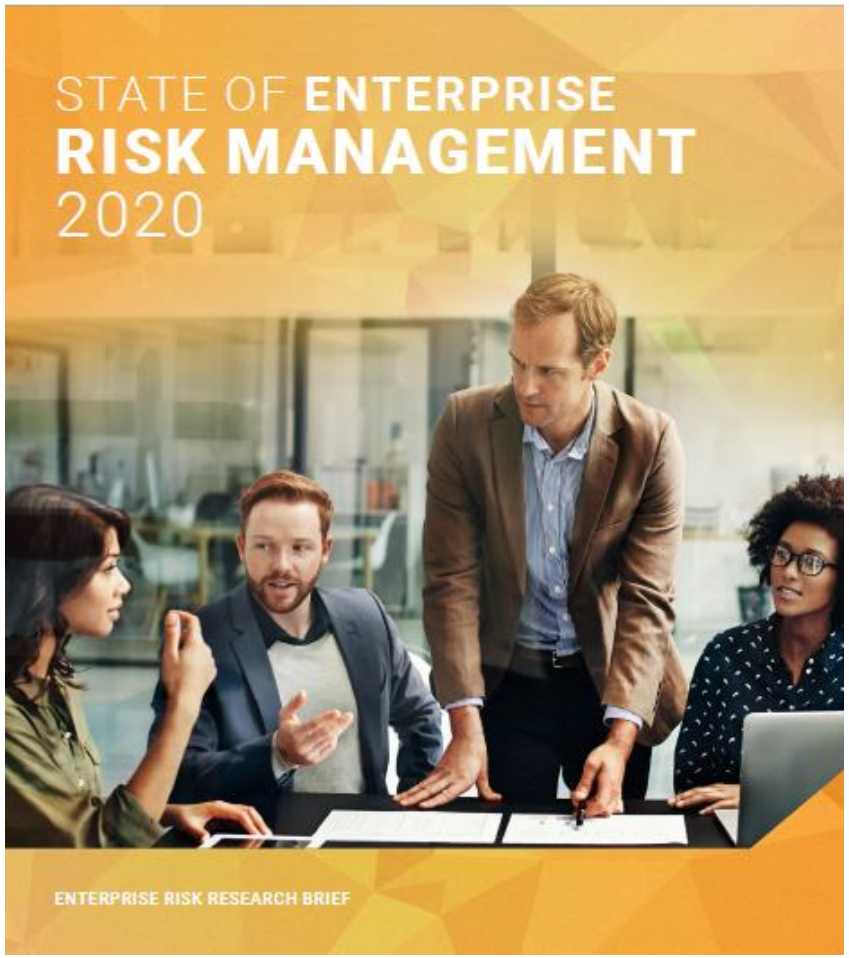
SSM Risk Map for 2019

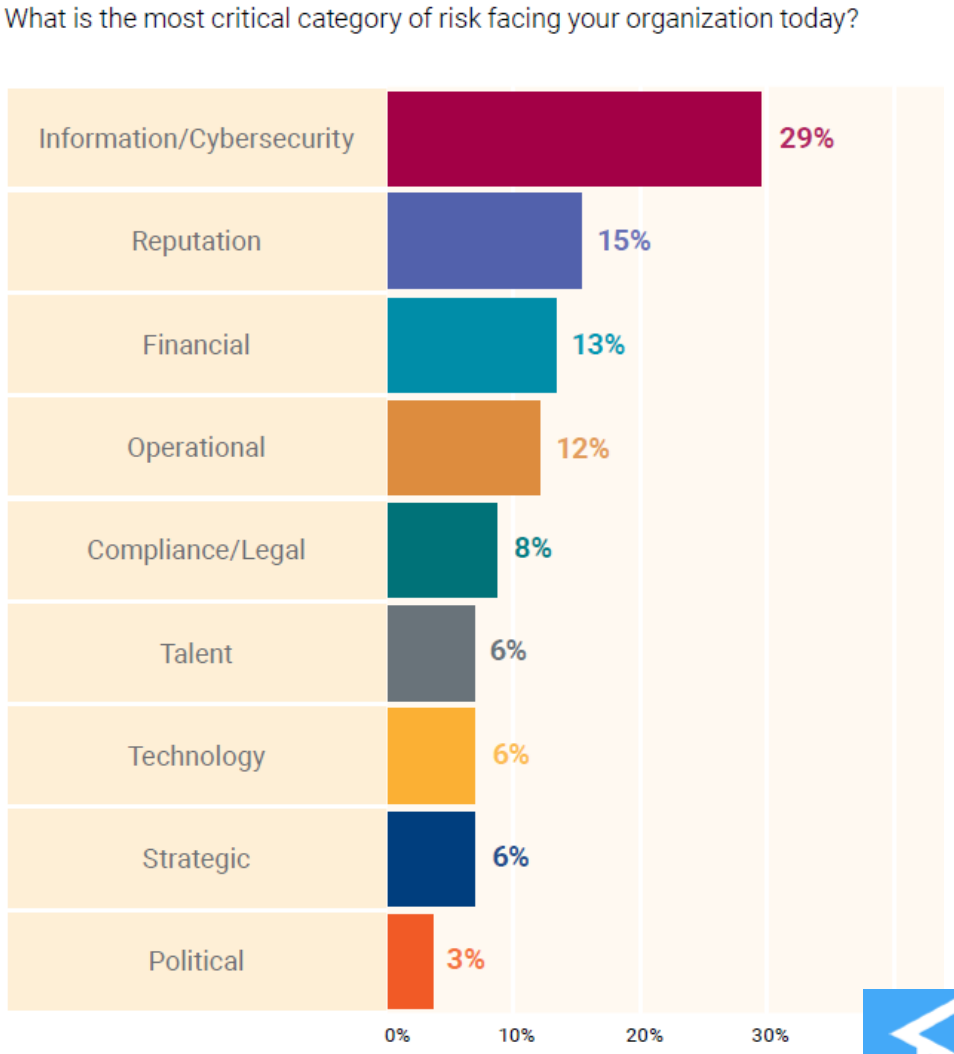



SSM Risk Map for 2020



# Рискът от киберсигурност е растящо и ключово предизвикателство



# Рискът – дефиниция

Възможността да възникне събитие, което да въздейства неблагоприятно върху **постигането на целите на организацията**. В тази връзка:

- ***Организацията определя ясни цели**, за да позволи идентифицирането и оценката на рисковете, свързани с целите;*
- ***Организацията идентифицира рисковете за постигането на целите** в целия обект и анализира рисковете като основа за определяне на това как трябва да се управляват рисковете;*
- ***Организацията идентифицира и прави оценка на промените**, които биха могли значително да повлияят на системата за вътрешен контрол.*

# Какво е киберриск?

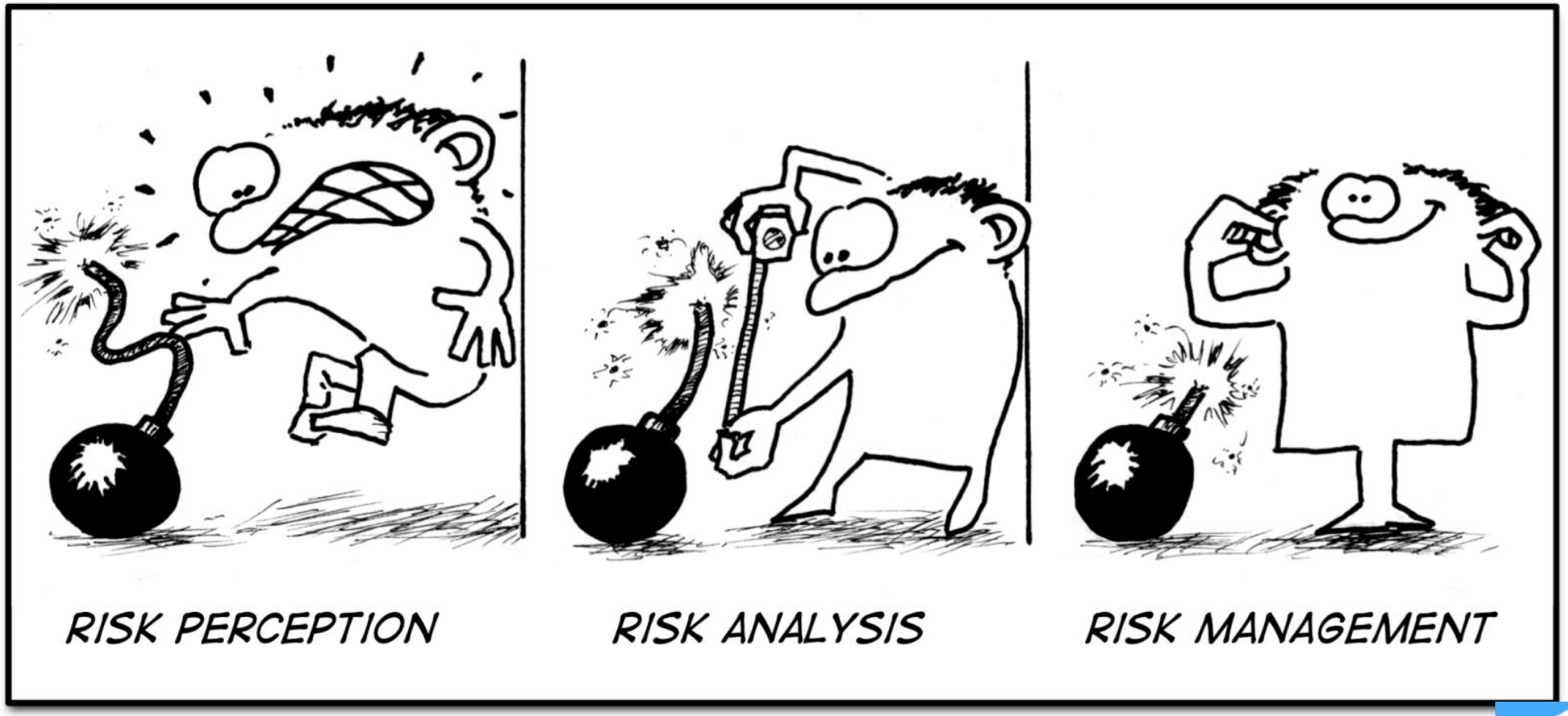
RISK CULTURE LAB

- Рискът за киберсигурност е вероятността от експозиция или загуба в резултат на кибератака или нарушаване на данните във вашата организация;
- Киберрискът обикновено се определя като излагане на вреда или загуба в резултат на нарушения или атаки на информационни системи. Въпреки това, това определение трябва да се разшири. По-добро, по-обхващащо определение е „потенциалът на загуба или вреда, свързана с техническите инфраструктура или използването на технологии в рамките на организацията";
- Рискът е възможността от реализиране на дадена заплаха и ефекта от нея. Рискът по отношение на сигурността на информацията се свързва с възможността заплахите да използват уязвимостите на информационен актив, причинявайки вреда на организацията.

SoftUni

# Процесът на управление на риска

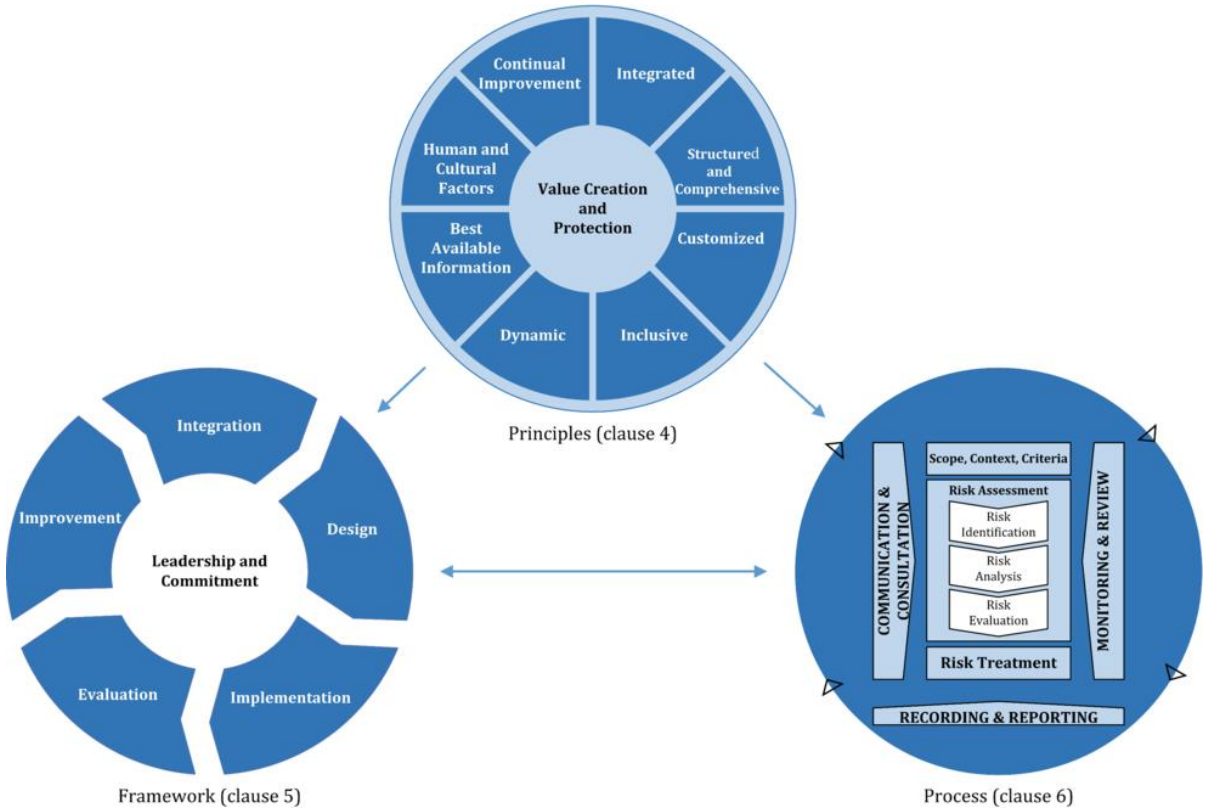
RISK CULTURE LAB




SoftUni

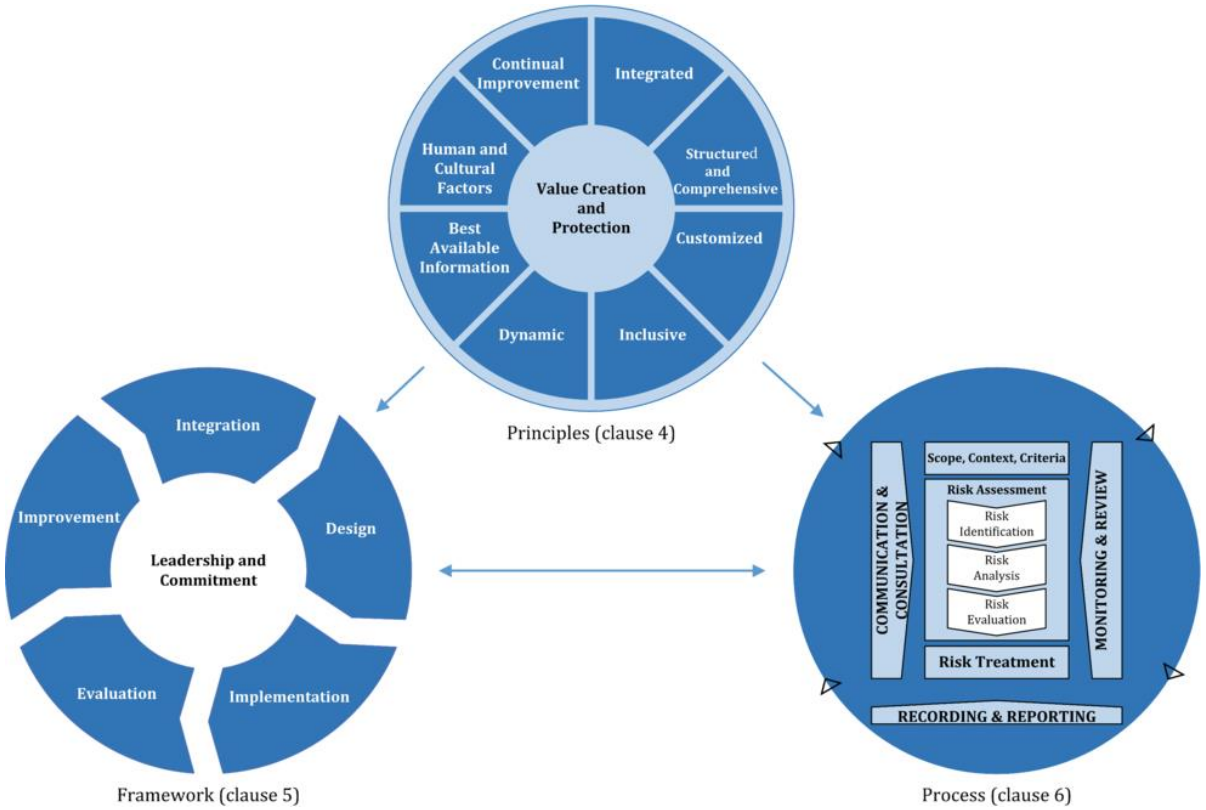
# Рамки за управление на риска

ISO/IEC 31000:2018




COSO ERM 2017

# Стандартът за управление на риска -ISO 31000:2018




- **Принципите** дават насоки за характеристиките на ефективното и ефикасно управление на риска;
- **Рамка за управление на риска** подпомага организацията за интегриране на управлението на рисковете във важни показатели и функции;
- **Процесът** на управление на риска включва систематично прилагане на политики, процедури и практики за дейностите по обсъждане и консултиране, установяване на контекста и оценка, третиранр, наблюдение, преглед, записване и докладване на риска.

# COSO ERM/2017

## Управление на риска в организациите

# Насоки на ЕБО относно управлението на риска от ИКТ и сигурността


Насоките определят как финансовите институции трябва да управляват ИКТ и рисковете за сигурността, на които са изложени, и да покриват следните области:

- Корпоративно управление и стратегия
- Рамка за управление на риска от ИКТ и сигурност
- Информационна сигурност
- Управление на ИКТ операции
- ИКТ проекти и управление на промените
- Управление на непрекъснатостта на бизнеса

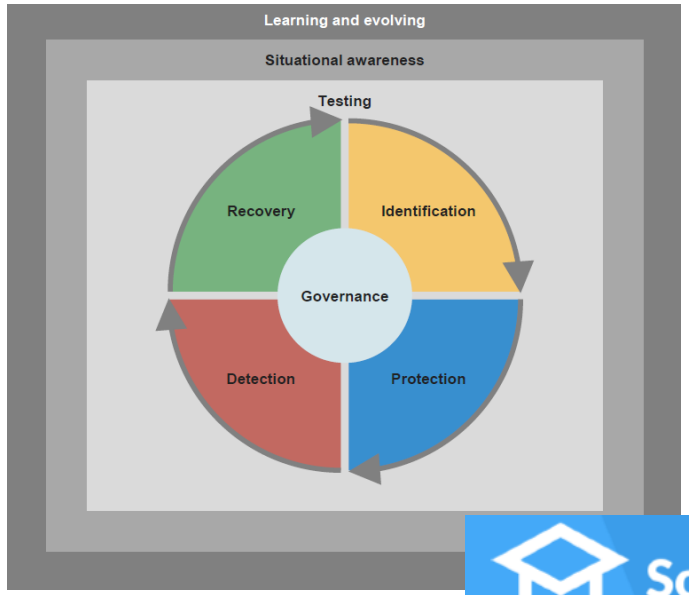
# Рамки за кибресигурност

NIST Cybersecurity Framework Version 1.1


ISO/IEC 27001

Information technology — Security techniques — Information security management systems — Requirements

Cyber resilience oversight expectations for financial market infrastructures



National Institute of Standards and Technology
U.S. Department of Commerce

RISK CULTURE LAB

# NIST Cybersecurity Framework Version 1.1/2018

SoftUni

# Рамката

Рамката предоставя обща таксономия и механизъм на организациите за:

1) Да опишат тяхната настояща позиция за киберсигурност;

2) Да опишат тяхното целево състояние за киберсигурност;

3) Определяне и приоритизиране на възможностите за подобрение в контекста на непрекъснат и повтарящ се процес;

4) Оценка на напредъка към целевото състояние;

5) Комуникация между вътрешни и външни заинтересовани страни относно риска от киберсигурност.

# Ядро на рамката

Елементите на ядрото на рамката работят заедно, както следва:

1) **Функциите** организират основните дейности по киберсигурност на най-високото им ниво;

2) **Категориите** са подразделения на функция на групи от резултати от киберсигурност, тясно свързани с програмните нужди и конкретни дейности;

3) **Подкатегориите** допълнително разделят една категория на конкретни резултати от технически и / или управленски дейности.;

4) **Информационните референции** са специфични раздели на стандарти, насоки и практики, често срещани сред критичните инфраструктурни сектори, които илюстрират метод за постигане на резултатите, свързани с всяка подкатегория.

# Рамката за киберсигурност и културата

RISK CULTURE LAB

- Петте основни основни функции трябва да се изпълняват едновременно и непрекъснато, за да формират оперативна култура, която да се справи с динамичния риск за киберсигурност.

- Управлението на риска на киберсигурност е част от **организационната култура** и е резултат от осведоменост за предишни дейности и непрекъсната информираност за дейностите в системите и мрежите на организацията. Организацията може бързо и ефективно да вземе предвид промените в целите на бизнеса / мисията в начина по който третира риска и осъществява комуникация за риска.


SoftUni

RISK CULTURE LAB

# ISO/IEC 27001

## Information technology — Security techniques — Information security management systems — Requirements

(Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания)

SoftUni

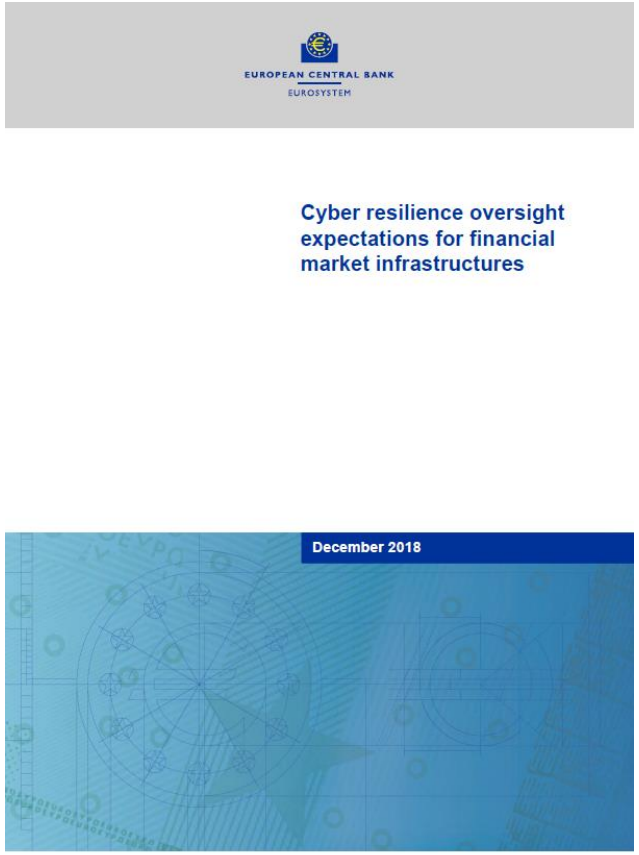
# ISO/IEC 27001Системи за управление на сигурността на информацията

RISK CULTURE LAB

- **Контекст на организацията**. Организацията разбира и взема предвид своята външна и вътрешна среда, очакванията и интересите на заинтересованите страни и дефинира обхвата на системата за информационна сигурност;
- **Лидерство**. Висшето ръководство демонстрира лидерство и ангажираност по отношение на системата за управление на сигурността на информацията, разработва политики за информационна сигурност и определя съответните роли и отговорности в организацията;
- **Планиране**. Организацията планира действия за да адресира рисковете и възможностите и разработва цели за информационна сигурност и планове за постигането им;
- **Осъществява поддържка**. Организацията определя и осигурява необходимите ресурси, компетенции и ниво на осведоменост на служителите, комуникации и документиране за създаването, внедряването, поддържането и непрекъснатото подобряване на системата за управление на сигурността на информацията;
- **Операции**. Организацията осъществява дейността си посредством оперативно планиране и контрол, оценка и третиране на риска за сигурност на информацията;
- **Оценяване на работните характеристики**. Организацията оценяава резултатите посредством мониторинг, измерване, анализ, оценяване и одит на работните характеристики на сигурността на информацията и ефикасността на системата за управление на сигурността на информацията;
- **Подобряване**. Организацията трябва непрекъснато да подобрява актуалността, адекватността и ефикасността на системата за управление на сигурността на информацията посредтвом коригиращи действия при несъответствие и чрез непрекъснато усъвършенстване.

SoftUni

# Надзорни очаквания за на кибер устойчивостта на инфраструктурите на финансовите пазари




# Полезни връзки

RISK CULTURE LAB

ISO 31000:2018 Risk management — Guidelines
https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
2017 Enterprise Risk Management – Integrated Framework
https://www.coso.org/Pages/default.aspx
https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf
NIST  Cybersecurity Framework Version 1.1
https://www.nist.gov/cyberframework/framework
SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements
https://www.iso.org/isoiec-27001-information-security.html
Cyber resilience oversight expectations for financial market infrastructures,
https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf
Managing cyber risk in a digital age
https://www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf
COBIT 2019 Framework: Introduction and Methodology,
https://www.isaca.org/bookstore/bookstore-cobit_19-digital/wcb19fim
Implementing the NIST Cybersecurity Framework Using COBIT 2019,
https://www.isaca.org/bookstore/bookstore-cobit_19-digital/wcb19nist

RISK CULTURE LAB

# Дизайн на културата на киберсигурност

**Светлозар Каранешев, Risk Culture Lab**

22 април, 2020

София

SoftUni

# Как работи културата

RISK CULTURE LAB

Културата като набор от базови допускания (ценности, приети за даденост) определя за нас на какво да обръщаме внимание, какво то означава, как да реагираме на това, което се случва и какви действия да предпиремаме в различните ситуации.

Ценностите определят всички аспекти на нашия живот: нашата морална преценка, нашите ракции спрямо другите, нашата ангажираност към лични и организационни цели. Ценностите:

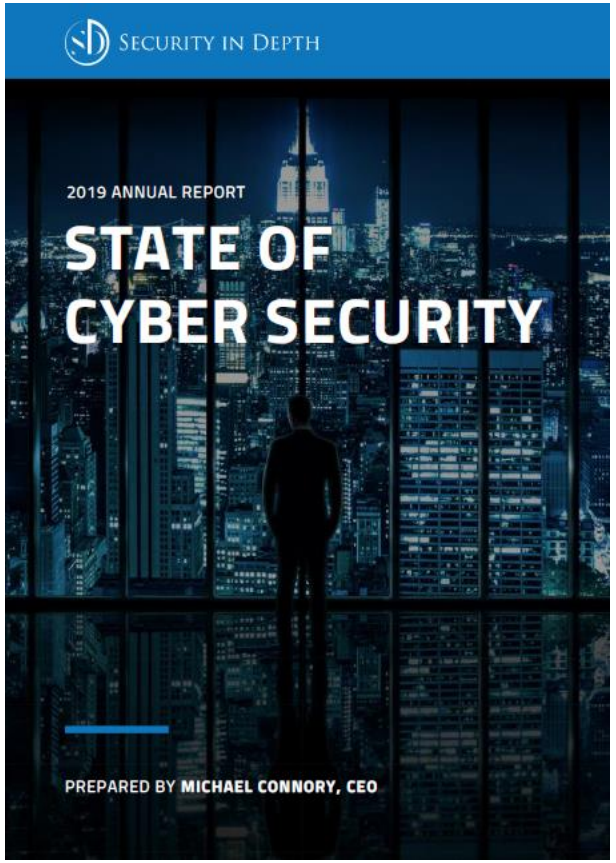
- Дават насоки за действия – те направляват нашите решения, какво да правим и какво не;
- Овластяват – когато ценностите са ясни, няма нужда от указания от висшестоящите какво да правим;
- Мотивират – карат ни да се фокусираме върху това защо правим, това, което правим и към целите, към които се стремим.

# Разходите за киберсигурност през 2019


Според Gartner световните разходи за продукти и услуги за информационна сигурност са 124 милиарда долара през 2019 г.

https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

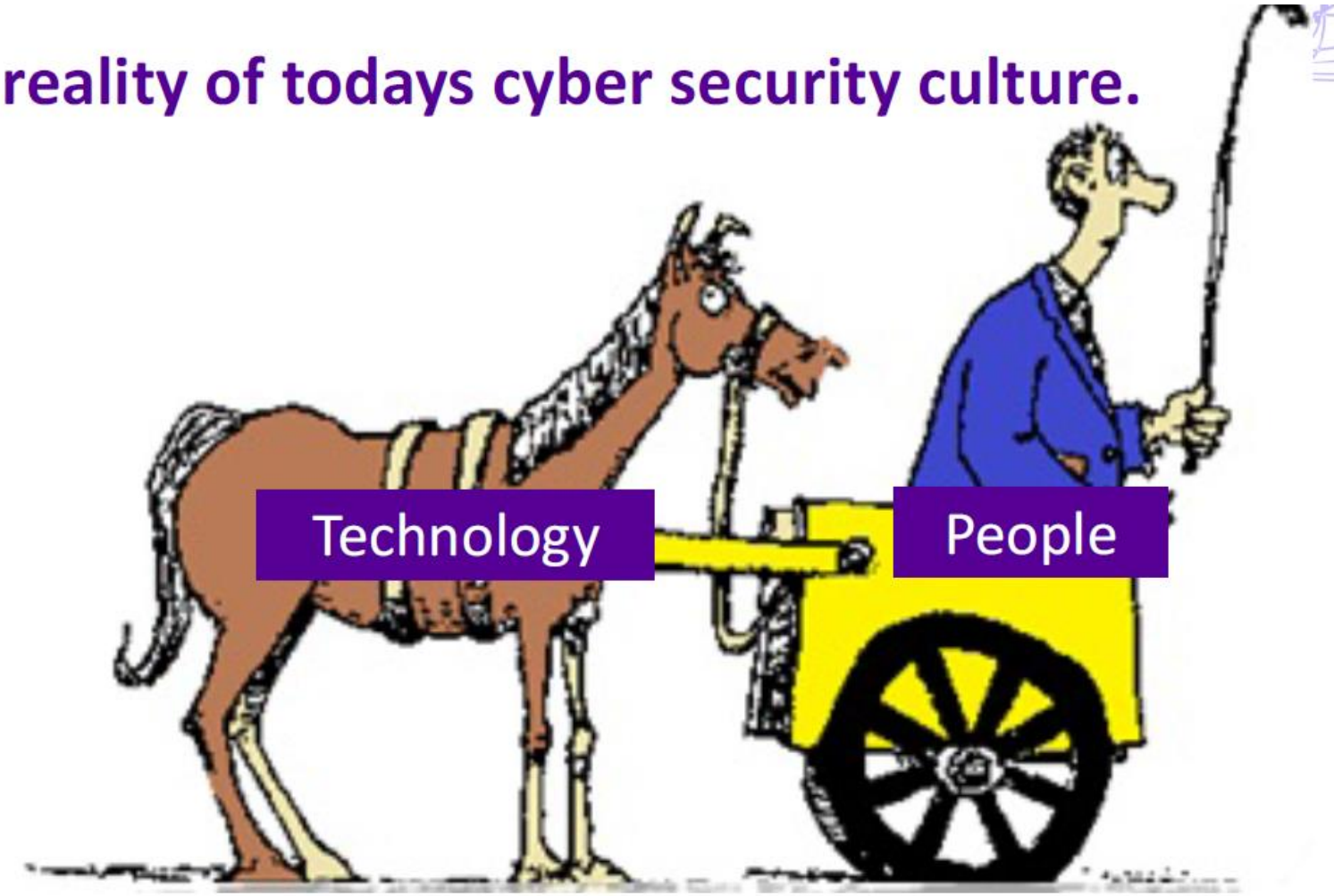
# Причината – човешка грешка




**70% от изтичанията на данни през 2019 година са причинени от човешка грешка**

RISK CULTURE LAB

# The reality of todays cyber security culture.




Technology should not be guiding your people, your people should be guiding your technology decisions.

SoftUni

RISK CULTURE LAB

## Прост тест – дали вашето пътуване за управление на културата на кибер сигурността е:

1. Непрекъснат процес на обучение, вграден в начина, по който се прави бизнес?
2. Отнася се за ценностите и поведението, свързани с киберсигурността?
3. Е в съответствие със стратегията за киберсигурност?

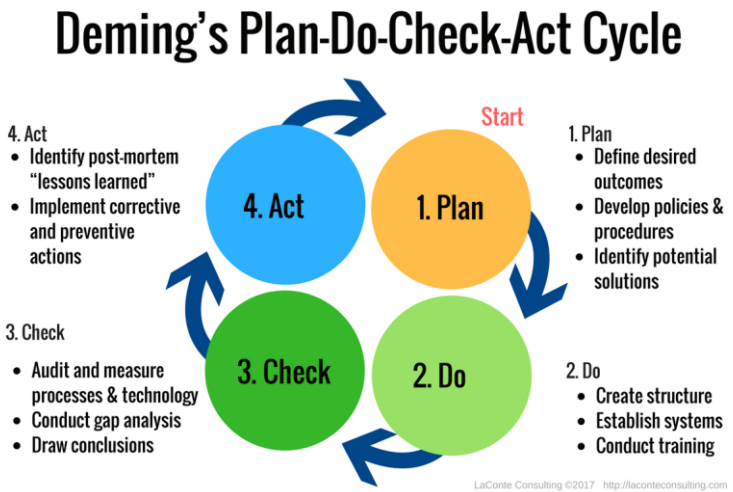
SoftUni

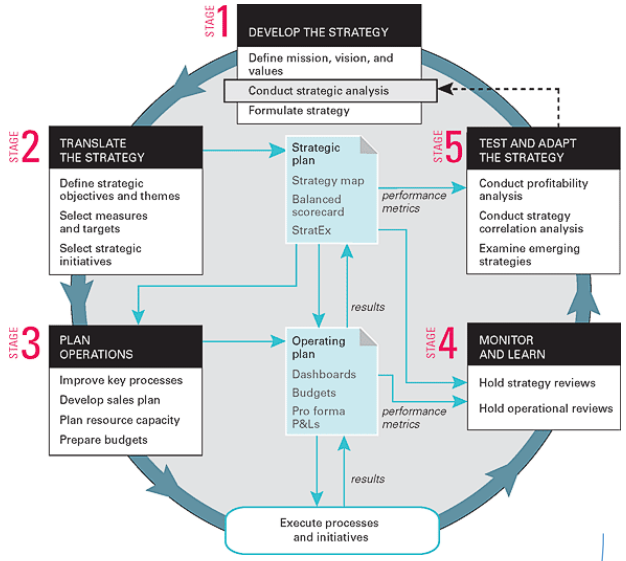
RISK CULTURE LAB

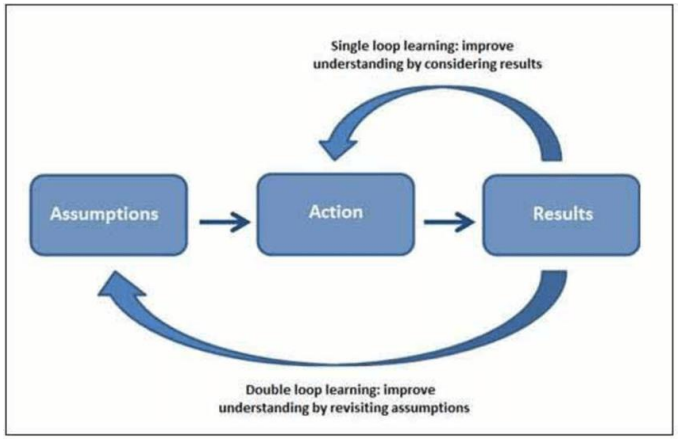
# Процес
# (метафората на градината)


SoftUni

# Какъв процес?

# Ценности и поведение (метафората за айсберга)

RISK CULTURE LAB

SoftUni

# Ценности и поведение

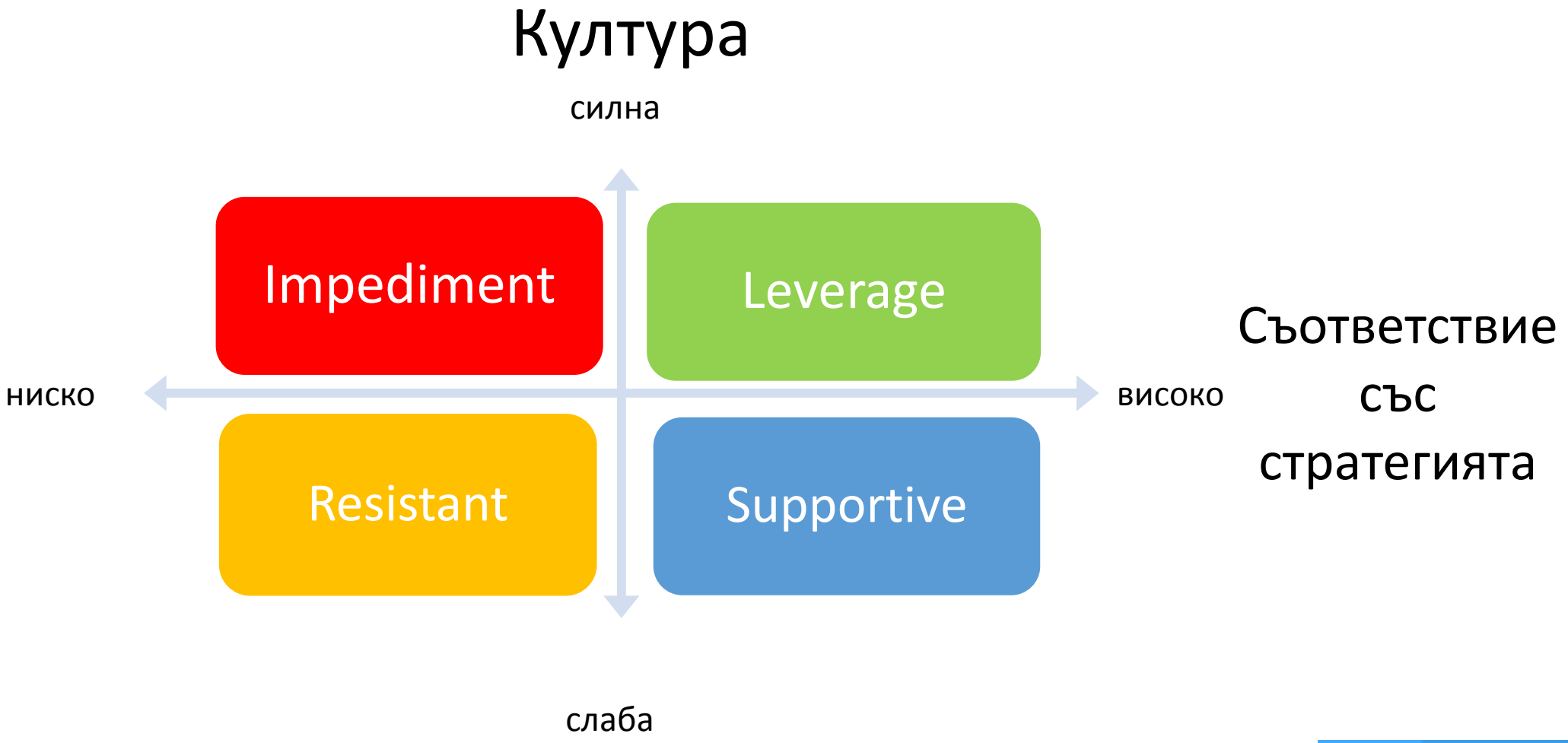

https://www.valuescentre.com/barrett-model/

RISK CULTURE LAB

# Съответствие със стратегията за киберсигурност (метафората за дървото)

SoftUni

# Културата изяжда стратегия за закуска



RISK CULTURE LAB

# Ако има поне един отговор с „не“, има проблем с управлението на културата на киберсигурност.

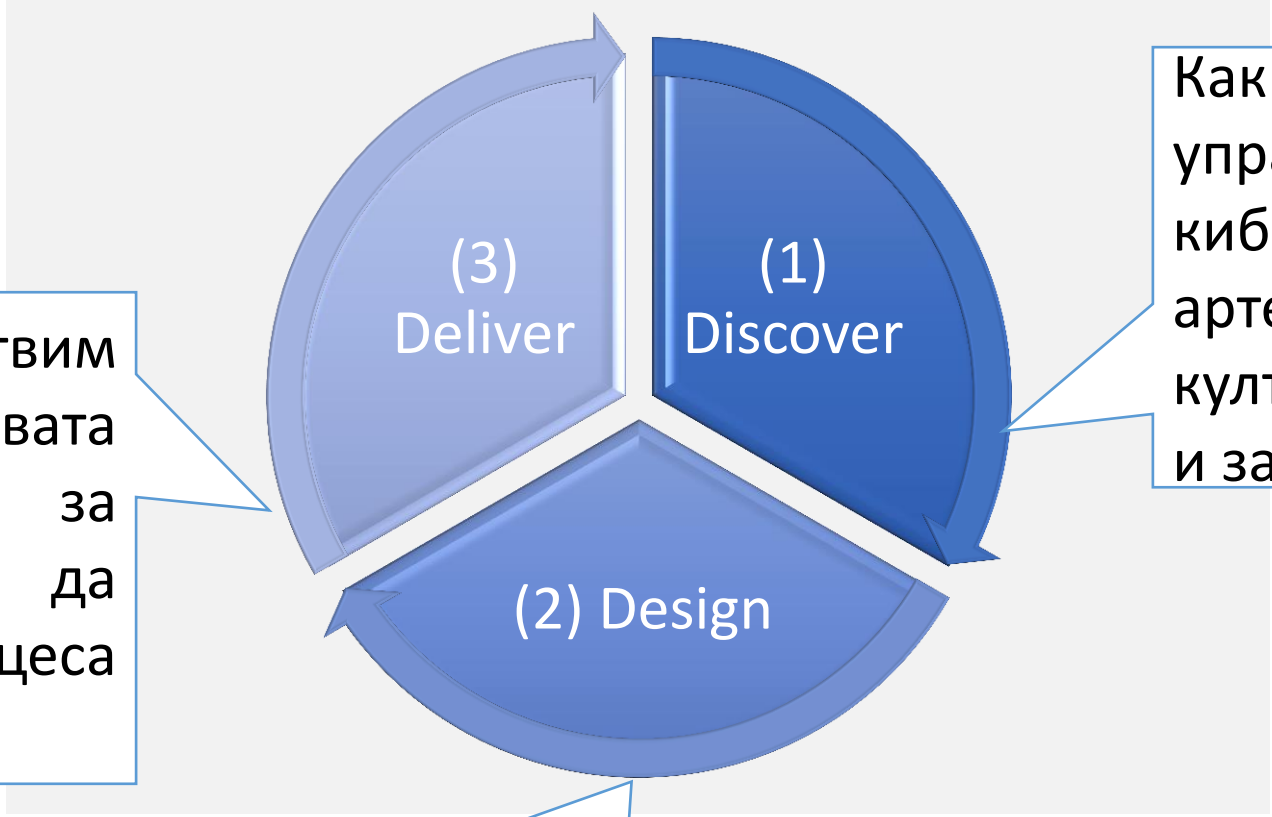
SoftUni

RISK CULTURE LAB

# Дизайн на културата на киберсигурност

# Дизайн на културата на киберсигурност –$D^3$ подхода

RISK CULTURE LAB




Какво правим при управлението на киберсигурността (какви са артефактите на нашата култура за киберсигурност) и защо?

Как да осъществим (изградим) целевата култура за киберсигурност и да направим процеса непрекъснат?

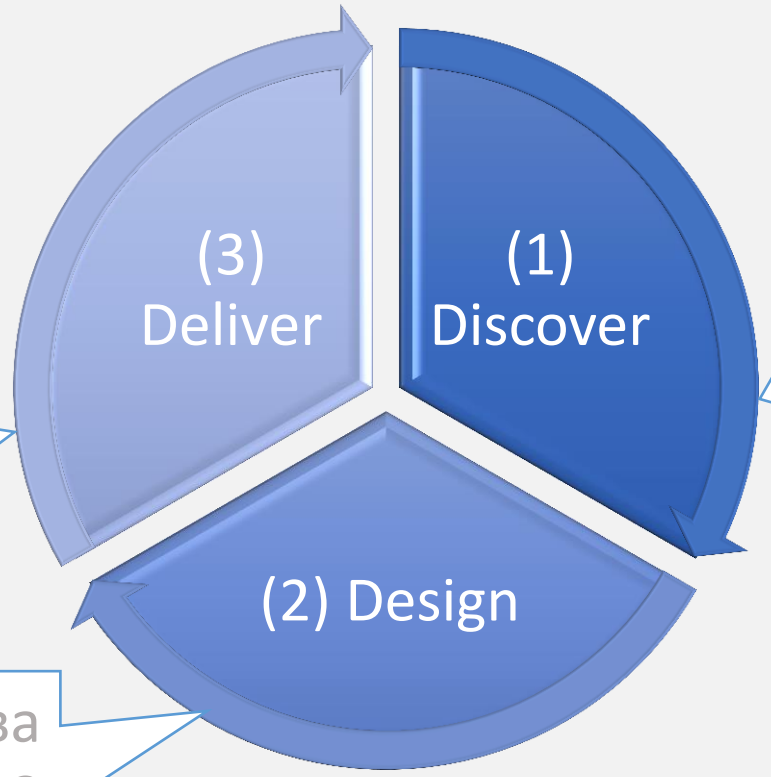
Каква е нашата целева култура за киберсигурност? Какво трябва да правим и защо?

SoftUni

# Дизайн на културата на киберсигурност –D3 подхода

RISK CULTURE LAB

Как да осъществим (изградим) целевата култура за киберсигурност и да направим процеса непрекъснат?




Каква е нашата целева култура за киберсигурност? Какво трябва да правим и защо?

Какво правим при управлението на киберсигурността?

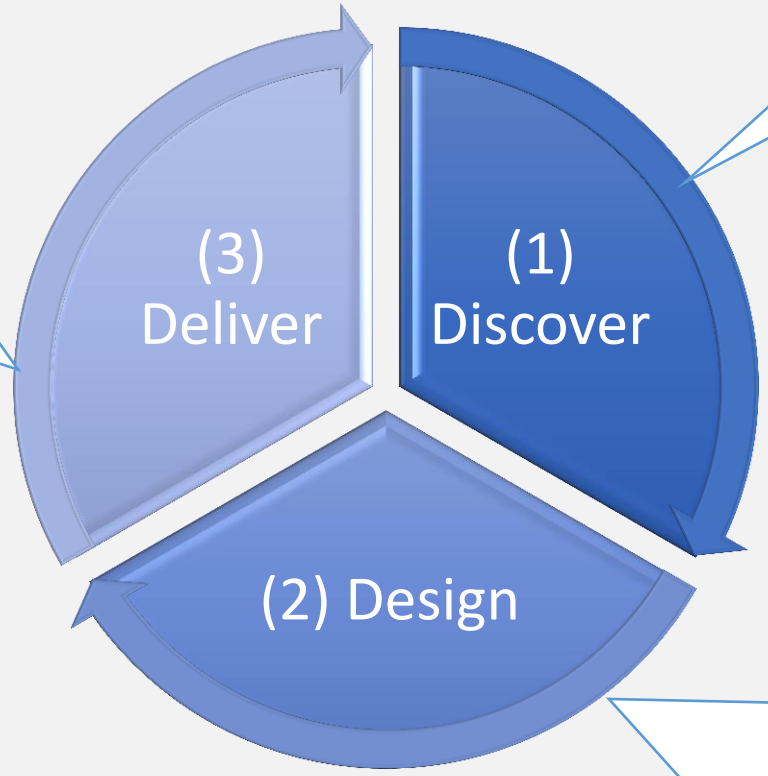
1. Анализ на контекста
2. Какво правим при управлението на киберсигурността (какви са артефактите на културата на киберсигурността)?
3. Защо правим нещата, които правим (какви са нашите ценности и дълбоки предположения)?
4. Какви са организационните условия?

SoftUni

# Дизайн на културата на киберсигурност –D3 подхода

RISK CULTURE LAB

Какво правим при управлението на киберсигурността (какви са артефактите на нашата култура за киберсигурност) и защо?




Как да осъществим (изградим) целевата култура за киберсигурност и да направим процеса непрекъснат?

1) **Каква е целевата култура за киберсигурност?**
2) **Какви са правилните поведения при управление на киберсигурността и какви ценности и предположения остават зад тях?**
3) **Какви са необходимите организационни условия?**

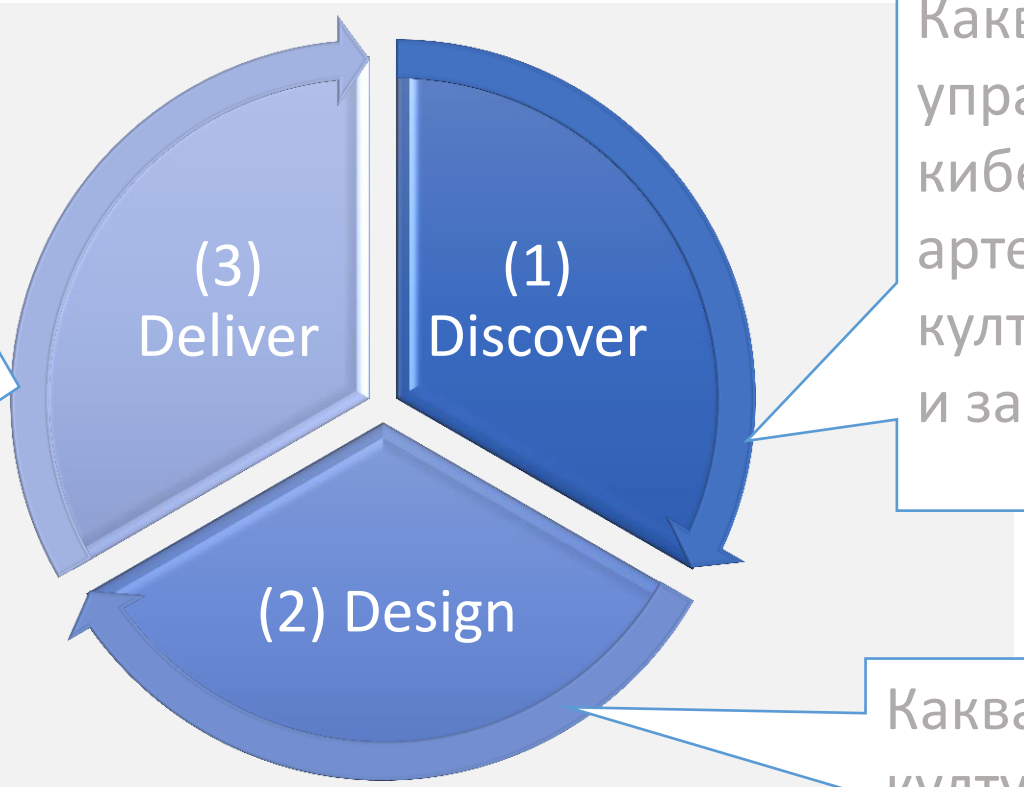
SoftUni

# Дизайн на културата на киберсигурност –D3 подхода

RISK CULTURE LAB

Как да осъществим (изградим) целевата култура за киберсигурност ?

1) **Какви инструменти да използваме, за да приложим предвидената култура за киберсигурност?**
2) **Как да планирате дейности**
3) **Как да разпределим ресурси**




Какво правим при управлението на киберсигурността (какви са артефактите на нашата култура за киберсигурност) и защо?

Каква е нашата целева култура за киберсигурност? Какво трябва да правим и защо?

SoftUni

# $D^3$ резултатите

RISK CULTURE LAB

$D^3$ Работилницата помага на екипите да разбират по-добре рисковете и да определят ценности и поведение свързани с риска. Това подобрява колективната способност на екипа да идентифицира, обсъжда и реагира на настоящите и бъдещите кибер-рискове на екипа.

Семинарът се основава на холистичен подход, който съчетава управление на риска и организационна култура и помага на екипите да идентифицират и разберат:

- С какви рискове се сблъсква екипът в ежедневните си дейности и каква е връзката на рисковете с целите и задачите на екипа;
- Поведение и взаимодействие на членовете на екипа по отношение на рисковете.
- Екипът споделя ценности и предположения зад поведението
- Как да открием стимулии препятствия за култура на риска и да определим ценности и поведение, които ще засилят капацитета на екипа за управление на рисковете
- Как да се разработят практики, които прилагат и засилват здравословна ри

SoftUni

# Благодаря за вниманието!

Светлозар Каранешев се занимава с оценка рисковете и ефективността на корпоративните и управленски системи, на критични бизнес и оперативни процеси и функции. Има над 25 години опит в сферата на риска и финансите. Съосновател е на Лаборатория по риск култура (Risk Culture Lab).

svetlozar.karaneshev@gmail.com

https://www.linkedin.com/in/svetlozar-karaneshev-59158713/