# Playing out your CISO role? Let's make it complicated!

Koen Fosse Matthys
Transcendent/FCG
Sikkerhetsfestivalen – Lillehammer- 2023

# TG/FCG is a leading governance, risk and compliance firm, offering best-in-class services and tech solutions to the European industry

## Founded 2008

FCG was founded in 2008 in Stockholm and has grown to become the leading Nordic advisor to businesses in Europe, having supported +700 clients of various size and business models.

## Experience

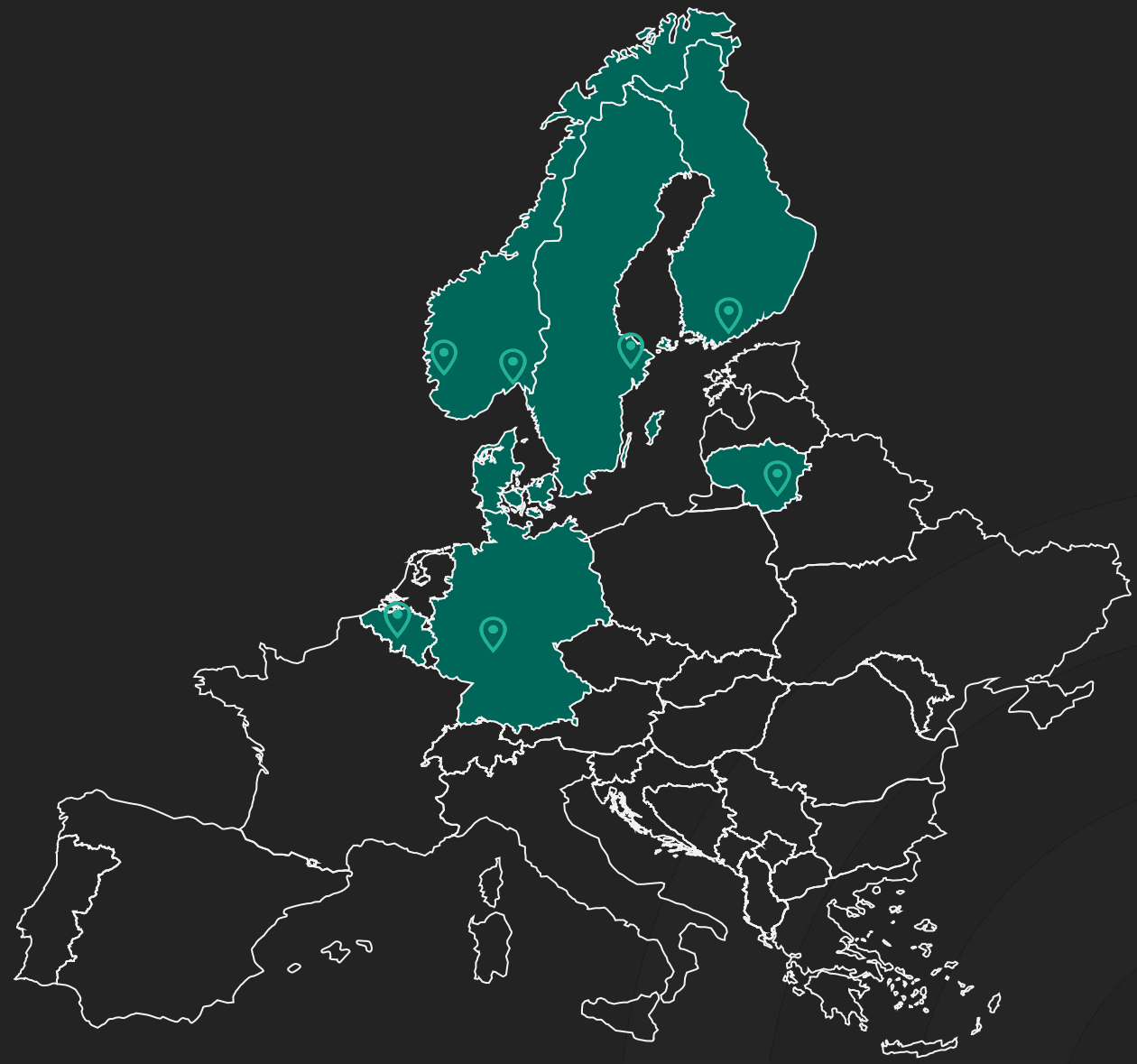
We are a Governance, Risk & Compliance Advisory / Services & Technology firm offering standard- or customized solutions depending on the client needs. FCG has a profound understanding of the challenges that our clients meet.

## +450 Employees

FCG has more than 450 employees and grows continuously.

## 10 Locations

Headquarter in Stockholm and offices in Gothenburg, Malmo, Copenhagen, Oslo, Bergen, Helsinki, Frankfurt, Brussels and Vilnius.



# Who am I?

Currently: Director/Head of Operational Resilience at Transcendent group/FCG Bergen

History:

Graduated Master of Research Information Science, specialization Gaming and Simulation (Hovedfag)

Gone through “the whole stack”, from developer/security operational to governance roles within security, IT and emergency

Experience from 3 different CISO roles a variety of sectors, mostly critical.

Extensive consulting, including CISO assist

Combining Cyber, process and emergency management for critical sectors.

Whoever believes in the generic CISO is wrong, we are humans with ambitions in complex and evolving organizations

# Why does this talk matter?

*Because a secure world needs good CISOs…*

*And because CISOs (are humans that) need to understand how they fill these shoes*

*Because we offer a safe playground to discuss/improve your CISO role*

# Precursor to this talk

- Newsletter internally “My first 100 days as a CISO - Group CISO? It’s complicated!” delivered an introspective view of my role as a CISO.

- Further reading provided more context:
  - Gartner – first 100 days as a CISO
  - Four CISO tribes and where to find them

- Some of the challenges were not only related to “Group CISO” configuration, but are universal (cross-domain, cross-organization). Let’s describe them!

- **This talk is not research**, this is an experience-based tool for discussion, improvement and insight in the execution of your role in a context

# Excuse me, what size are those CISO shoes?

- Two main factors influence how you perform in your role as a CISO:
  - Yourself as a person (including your ambitions)
  - The context in which you configure the CISO role (including its ambitions)

- Sometimes these factors can be influenced easily:
  - Obtaining budget to grow your organization during organizational growth
  - Convincing management commitment for security governance after an incident

- Sometimes, these factors can be hard to change
  - Your organizational position (f.eks. Within IT or internal status) is complicated to change
  - You lack the human skills for the role

# A tale of four tribes?

- Synopsis* did some very interesting research based on a field study of 25 CISOs in international organisations

- According to the research, all CISO could be divided into 4 tribes:
  - The Security as an Enabler-Tribe
  - The Security as Technology-Tribe
  - The Security as Compliance-Tribe
  - The Security as a Cost Center-Tribe

- Identified gap with regard to this research:  CISO and security professionals can be…

  - None of the four (Failed roles, f.eks. The Token CISO)
  - Combination of Tribe(s), organization and personality
  - In local context (Norway), CISO-roles are often combined with many other roles that share governance aspects (f.eks. CISO + CSO, CISO + CIO….)

Synopsis (1997): Four CISO tribes and where to find them. By G. McGraw, Sammy Migues, Brian Chess.

# Why not use the structure of a game?

- Games and simulations offer the perfect playground for learning and experimentation
- Why not play out archetypes of CISO roles together with peers?
  - Mirror function, communication tool
  - Safe feedback
- Goal of the game: Experiment with CISO role, share experiences in a safe context (What I would do…, what I have experienced…)

# How will it be played

- Three type of cards:
  - CISO archetype card
  - Situational card
  - Booster card (both positive and negative)
- For each round we start with the archetype – what are its challenges, what are you?
- Secondly, we add a situation that can help/impede you in your role execution
- Thirdly, other participants can add boosters
- Open form game without winners or scores

# Let’s try?

- Which one shall we pick?
  - The buried-deep-down CISO
  - The Token CISO
  - An Englishman in New York – CISO
  - The King without a country - CISO
  - The DIY operations – CISO

- Let’s expose these roles to situations within
  - Workforce
  - Governance
  - Controls

Use of force fields (tribal, SWOT,…)

# Role card - CISO (Tribe: N/A)

Internal strength

External threats

About your current position in the company

Internal weaknesses

External opportunities

# The “buried-deep-down” CISO (Tribe: Cost Center)

Probably you have operational insight and closeness to processes. Some budget influence.

You are placed deep down in the organizational structure, in the compliance, IT or Safety department, more than 1 level away from decision makers. You have no reporting link to EMT and no requests from the board or management on cyber risk or state of security. You can only influence through a subdivision’s budget and dependent on their priorities.

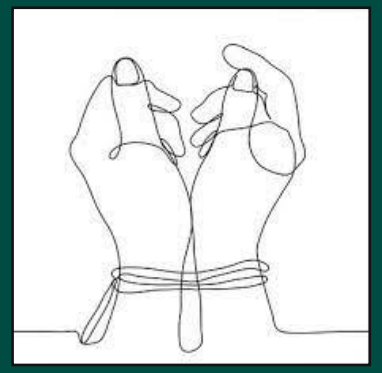
If your manager is risk aware, he or she will take your agenda to EMT/level up. Possibility to take several roles?

You might not be in touch with the real issues in EMT (Security Strategy // business?).

A cut in budget for a different domain (IT, risk) might cut your security budget

# The “Token CISO” (Tribe: None)

Plenty of time for conferences, talks, networking and courses!



You are engaged in your role because your organization wants to show stakeholders, customers or authorities that they have a go-to person, but your colleagues or management are actually not interested in improving cyber or building a security culture. You feel you are in a symbolic role with little influence

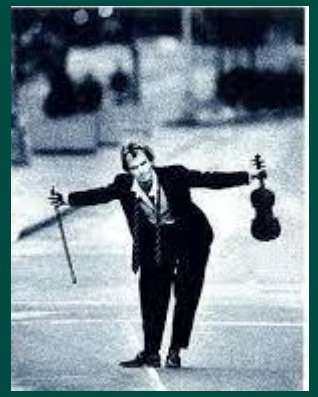
Lacking involvement in important decisions may lead to a vicious circle

Your role is (meant to be) powerless

Start with security culture (ground work) and risk matrix

# “An Englishman in New York” – CISO (Tribe: compliance /None)

You can enrich your C-level colleagues with your unique security and risk approach



You are high-level CISO surrounded by blue collar C-suite professionals that are too busy to talk about security or not interested in the topic. There is a considerable distance between you and operational security resources, and within your context, you are the odd duck in the bite, surrounded by white collars.

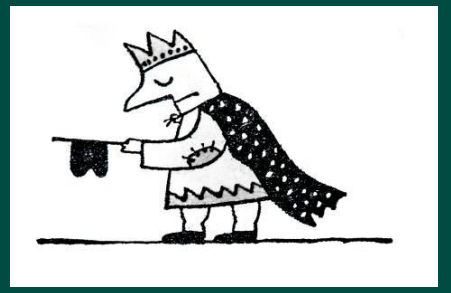
Aligning with business risk and security culture to the board room should be possible

You might not be talking the C-level speak or be too technical/ security oriented

Keep in touch with operations and emerging security risk (bottom up)

# The “King/Queen without a country”- CISO (Tribe: Compliance, Cost Center)

Your requirements are heard, you have the authority to enforce compliance



You have the right mandate and skills to develop policies, requirements. Your role as a requirements owner has put you outside the relevant (eks. IT, SecOps) department, which also has the main budget and prioritization. A king without land, your work might have little impact as it lacks implementation context

Align with other Kings/Queens and do compliance together Focus on audit and culture, and the rest will follow

You have mandate but no money or project ownership – how do you back your requirements?

Motivational fatigue when your country stays poor in security

# The DIY – CISO (Tribe: Technology)

You know how things are done, can verify, and even DO stuff in the baseline

You have come from a technical role and were promoted into a newly established Security Governance role in the company. You are hands-on and very close to operations, but far from management, audit and company risks. You are unfamiliar with the political side of the job and the associated mindset/approach

You can approach security both bottom up/top down if you learn both approaches

You are too tech for EMT and board room, and communicate best in projects/ technical level

If you do not master the GRC approach, governance will not happen

# The Convincer –CISO (Tribe: Enabler)

You create a framework for security and drive a strong security culture at all levels, which will bring compliance, security champions, …

You might be out of touch with what is happening at security operations and IRT/emergency management

You were engaged as a CISO because of your leadership and communication skills, and you are the go-to person for security advice, awareness and high-level security risks. You represent the company at network events, and are the perfect ambassador

Use security champions in order to focus on other governance areas

You might get quickly tired the repetitive or boring tasks such deviations, requirement documents and reporting

# Situation cards

Major security incident and its handling shows weak incident response and absence of resilience capability

Your company needs to become compliant with the NIS2 Information Security regulation within 9 months

You found a mentor from another company that you can spar with regarding difficult situations

The Board of Executives wants you to come to the board meeting and brief about current cyber risks for your sector

Your role is new and you can still shape it as you like, both with regard to operations and governance

Group management is considering change governance the model and remove the CISO role

# Booster cards (both negative and positive)

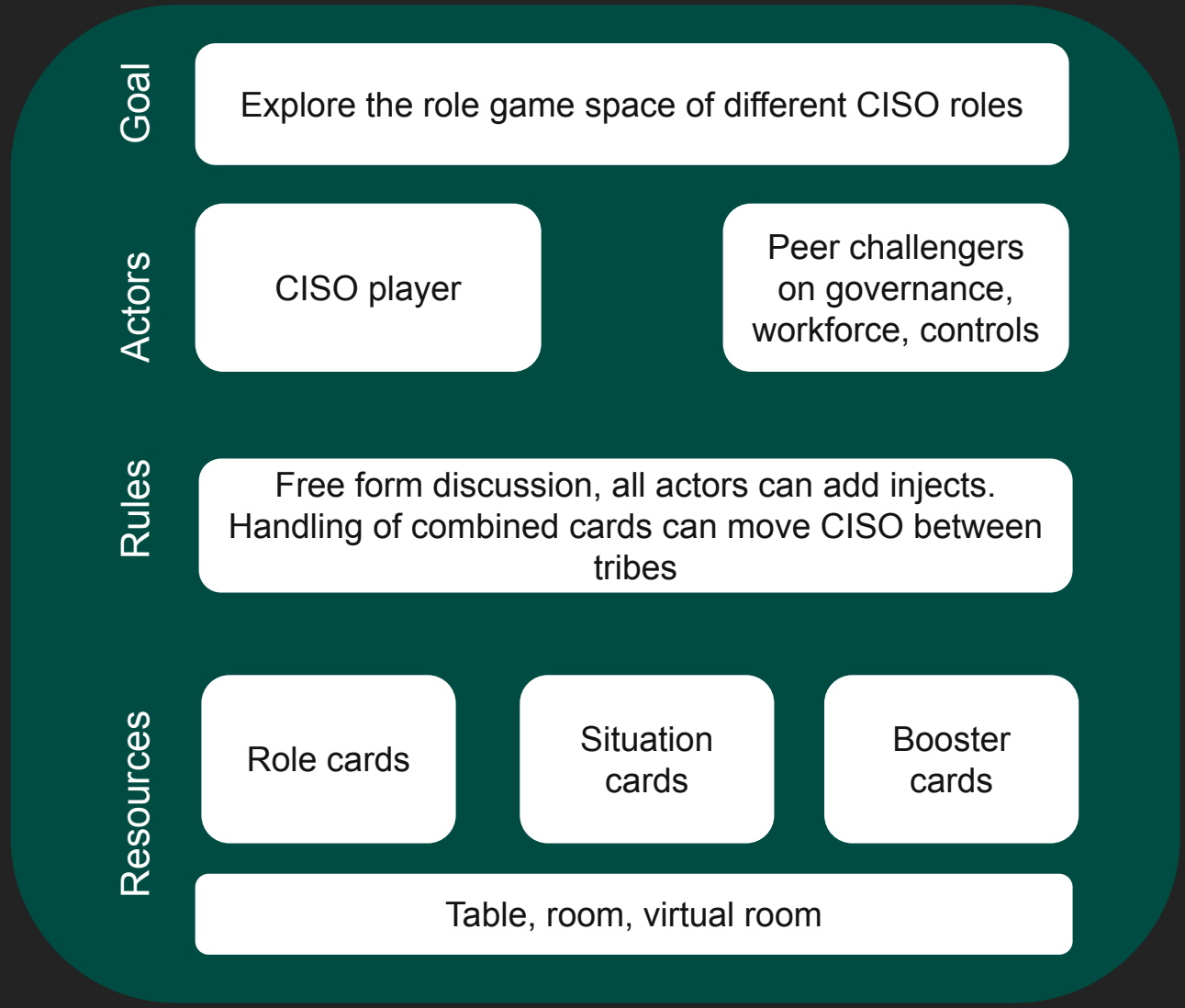
Your IT-provider asks for security requirements – an excellent opportunity to share risks and build trust

You found a mentor from another company that you can spar with regarding difficult situations

Your predecessor did a lousy job and did not care about culture or governance

Your company has an OT department, but you have no security governance here

# Summarized: Game structure



# How/where will this work?

- Gamification aspect
  - Can it be played? (Board, levels, points?)
  - Mainly meant as a communication tool between colleagues or within teams, mediate your “state” of CISO and get advice by peers
- Playable for a CISO round table, sector-CERT or IT-/IT-security team internally
- Can be used for other roles as well (Archetypes):
  - CIO, CSO
  - Safety, emergency manager
  - Quality role
- Game structure is free to use!
  - Any suggestions for improvement?

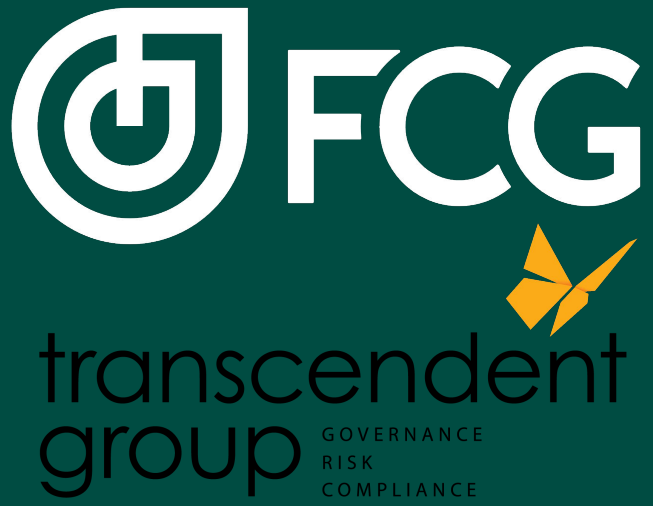
# Some conclusions

- Some important factors that form your CISO role are in YOUR hands
  - Do not start of blaming the organisation, its culture or your position
  - Leadership is a key feature of a well-functioning governance function
- This is not just a snakes and ladders game
  - Your personality and ambitions will influence your execution of the role
  - Your organization might need a certain type of CISO (What are you looking for?)

- During recruitment, both sides of the table should make sure to provide the right questions (and answers)

- Contact me if you want to play!

koen.matthys@transcendentgroup.com or LinkedIn


FCG
transcendent
group
GOVERNANCE
RISK
COMPLIANCE