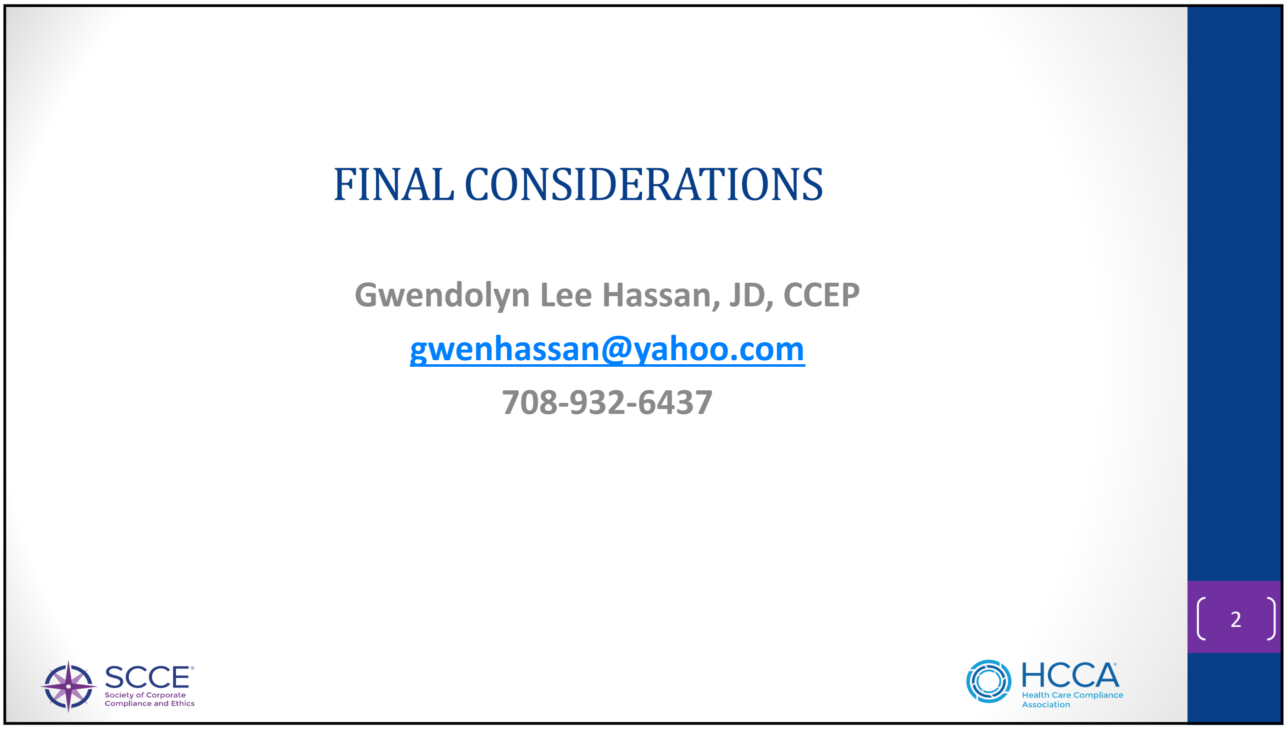
Compliance Risk Assessment and Management Workshop

Society of Corporate Compliance and Ethics and Health Care Compliance Association

1

1



FINAL CONSIDERATIONS

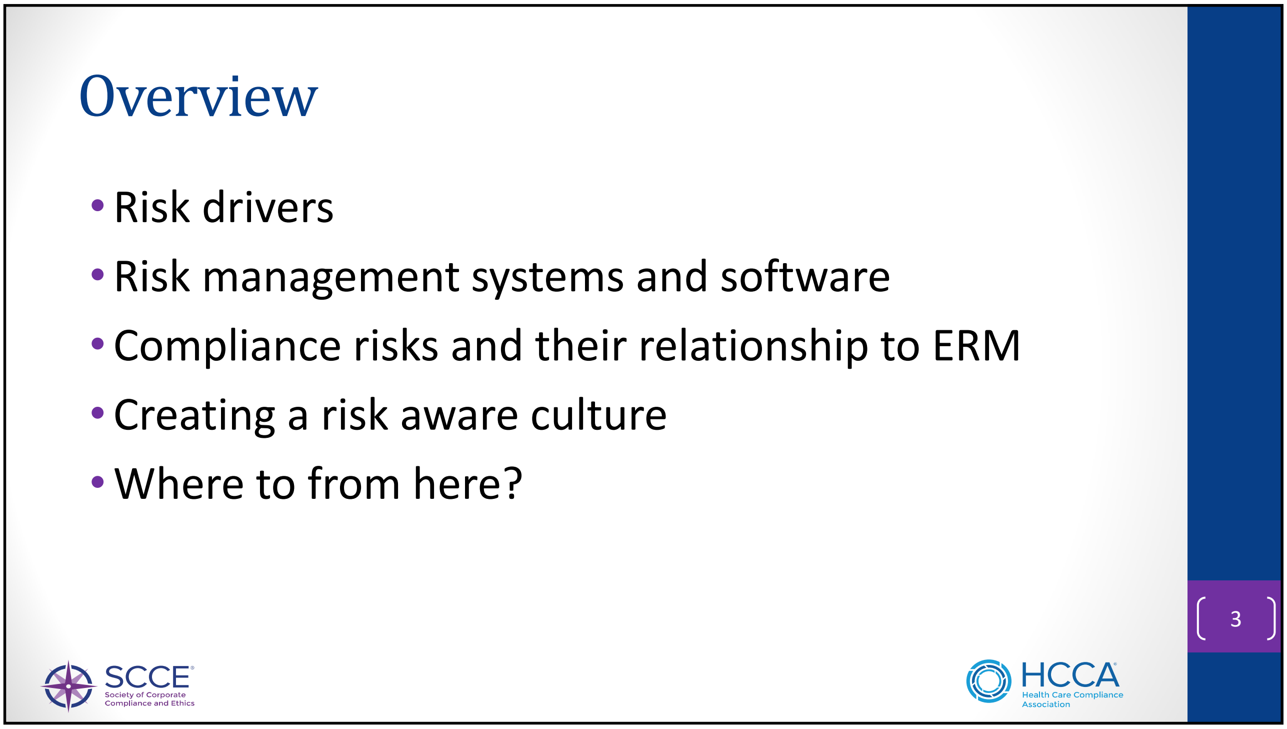
Gwendolyn Lee Hassan, JD, CCEP

gwenhassan@yahoo.com

708-932-6437

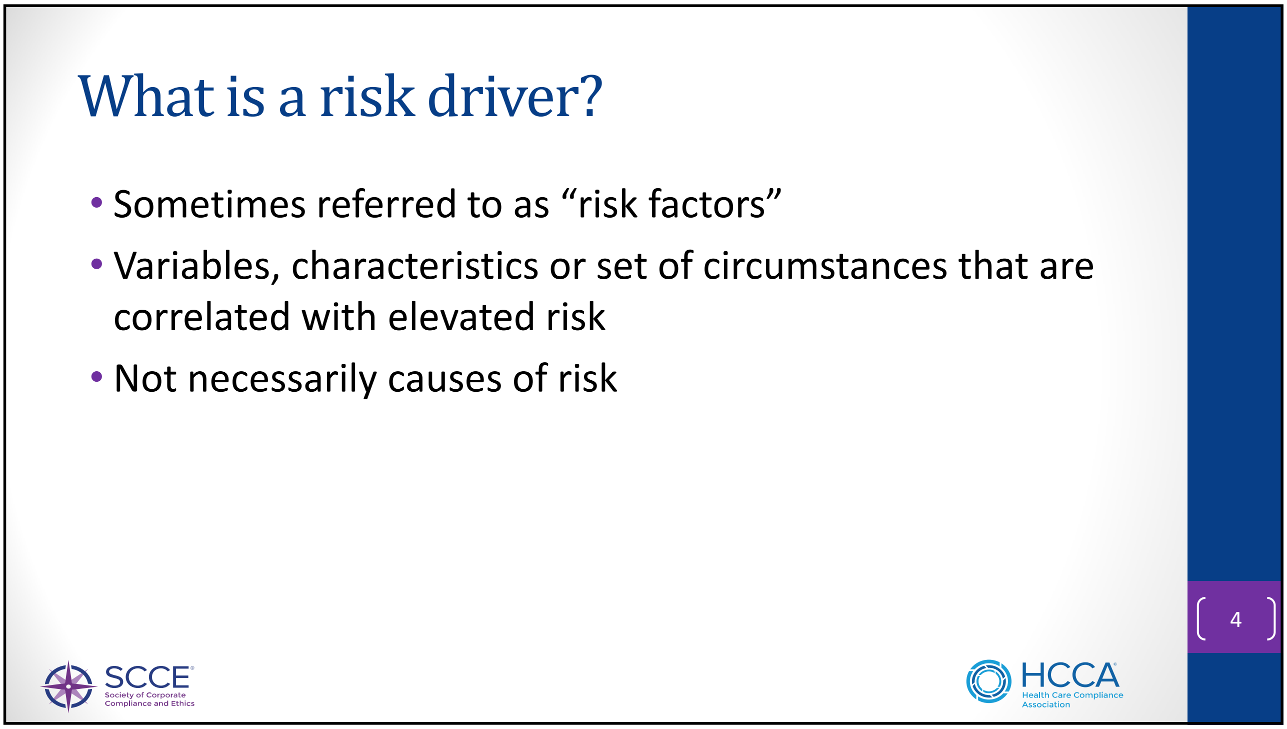
2

2



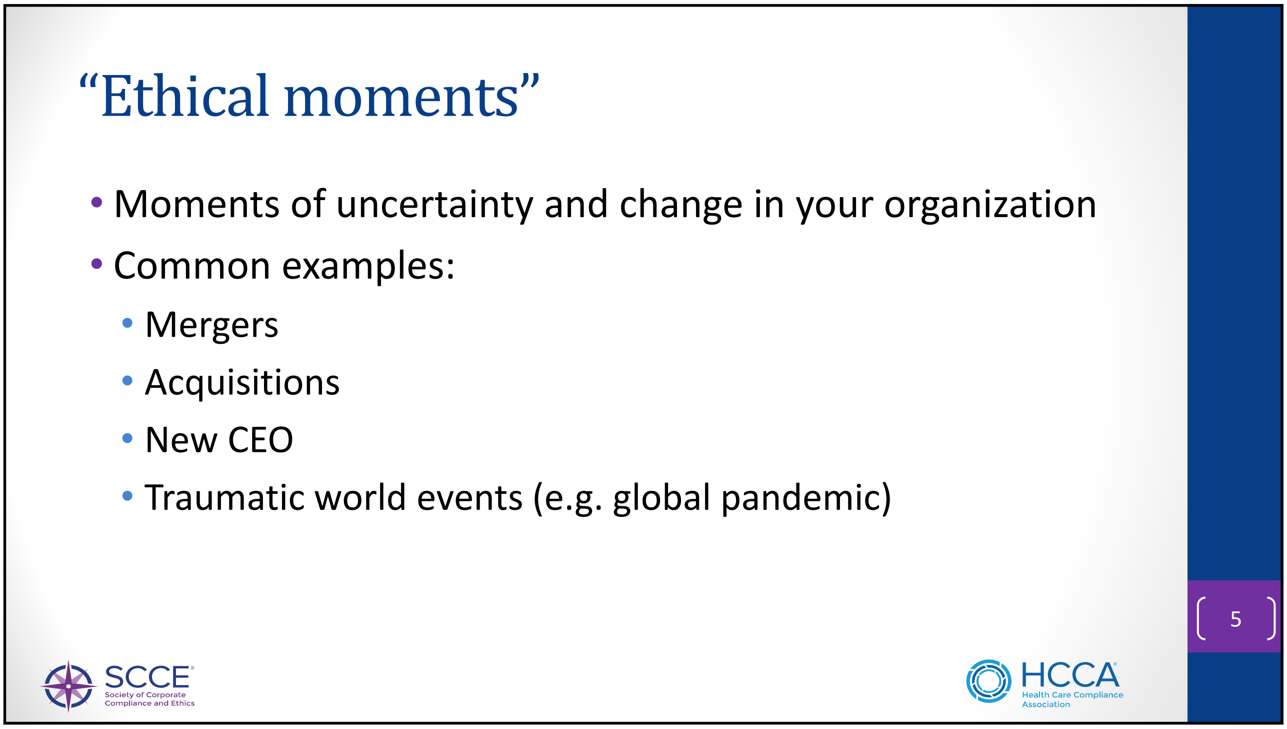
Overview

- Risk drivers
- Risk management systems and software
- Compliance risks and their relationship to ERM
- Creating a risk aware culture
- Where to from here?



What is a risk driver?

- Sometimes referred to as “risk factors”
- Variables, characteristics or set of circumstances that are correlated with elevated risk
- Not necessarily causes of risk

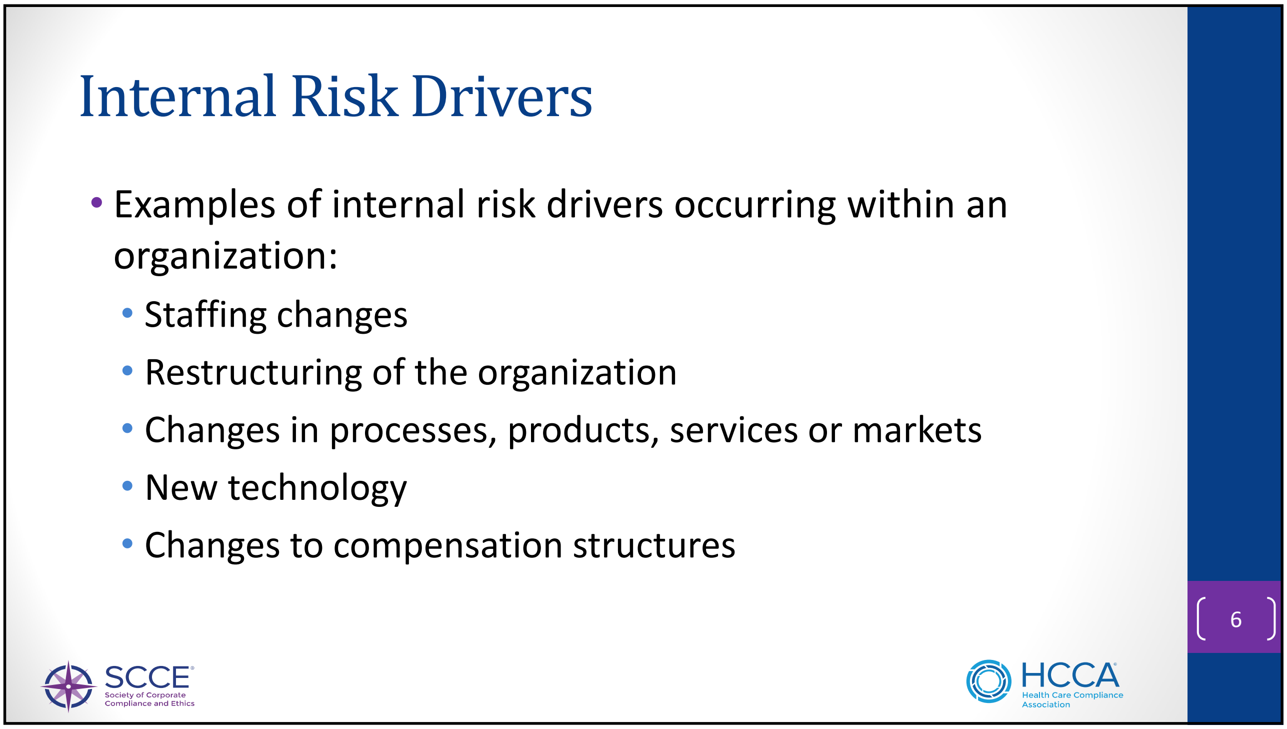


“Ethical moments”

- Moments of uncertainty and change in your organization
- Common examples:
  - Mergers
  - Acquisitions
  - New CEO
  - Traumatic world events (e.g. global pandemic)

5

5

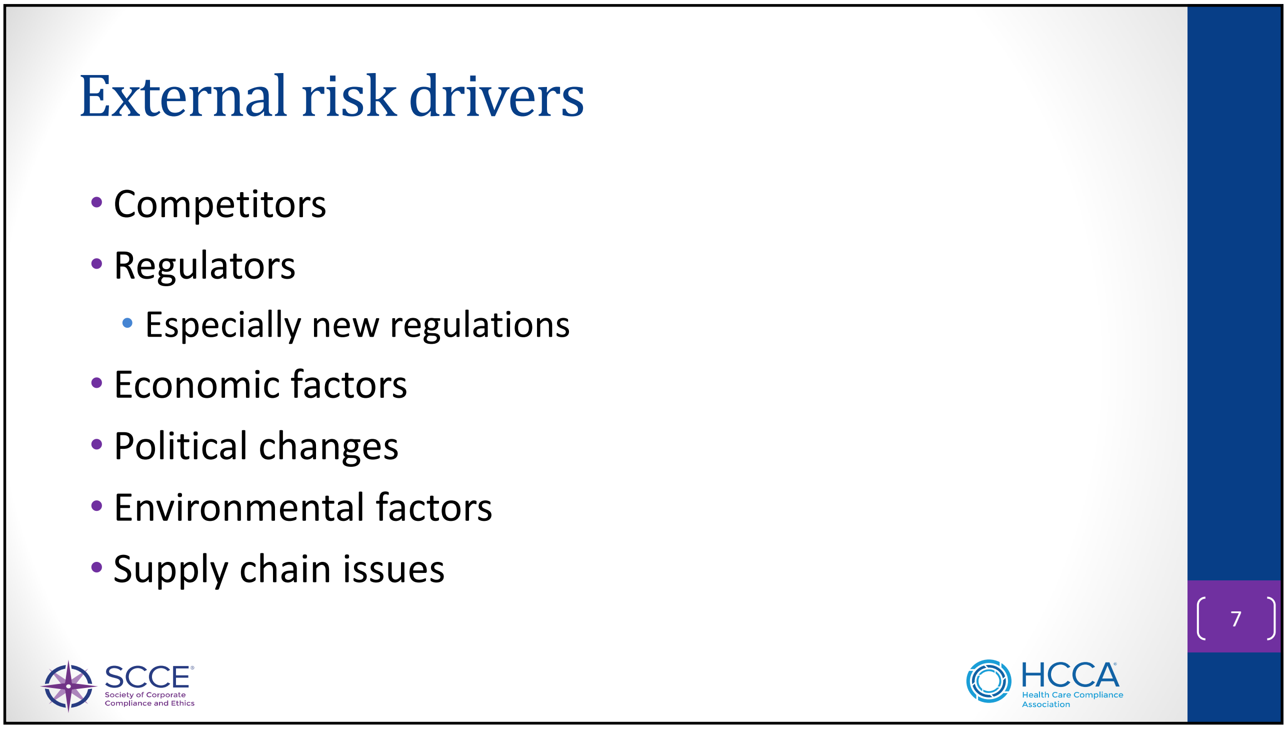


Internal Risk Drivers

- Examples of internal risk drivers occurring within an organization:
  - Staffing changes
  - Restructuring of the organization
  - Changes in processes, products, services or markets
  - New technology
  - Changes to compensation structures

6

6

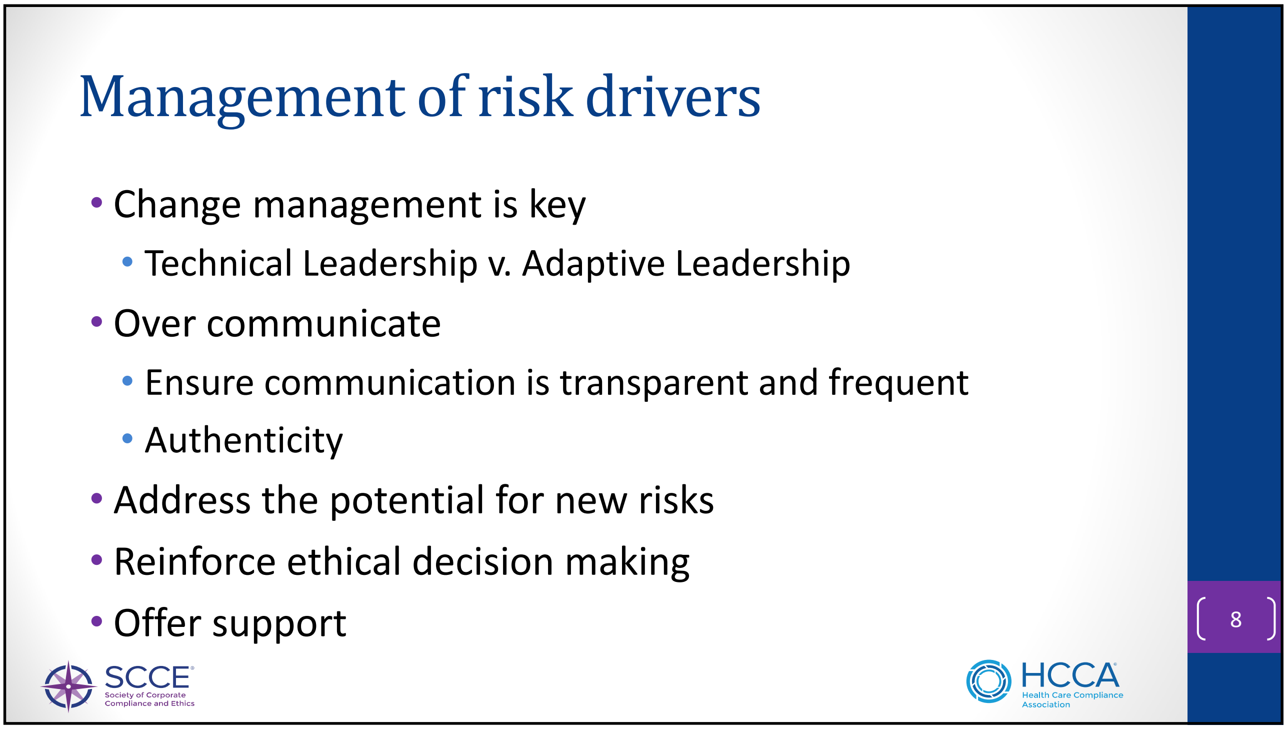


External risk drivers

- Competitors
- Regulators
  - Especially new regulations
- Economic factors
- Political changes
- Environmental factors
- Supply chain issues

7

7

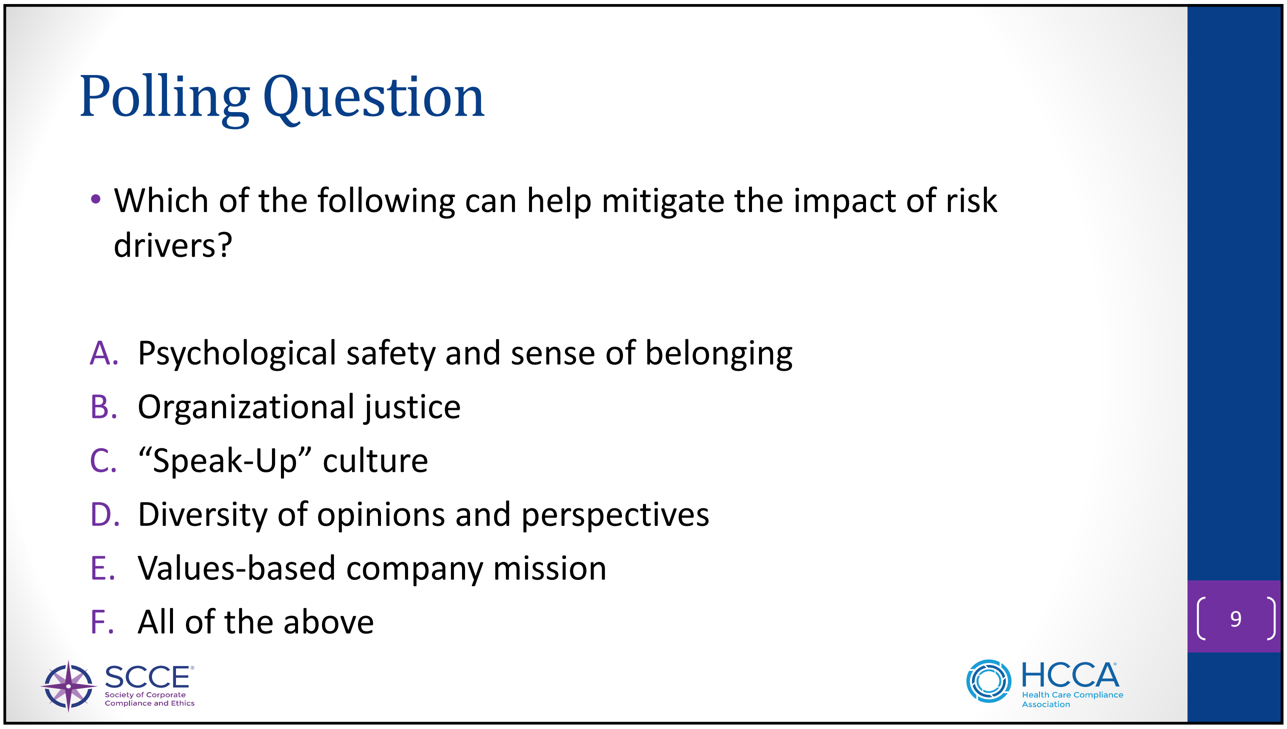


Management of risk drivers

- Change management is key
  - Technical Leadership v. Adaptive Leadership
- Over communicate
  - Ensure communication is transparent and frequent
  - Authenticity
- Address the potential for new risks
- Reinforce ethical decision making
- Offer support

8

8



Polling Question

- Which of the following can help mitigate the impact of risk drivers?

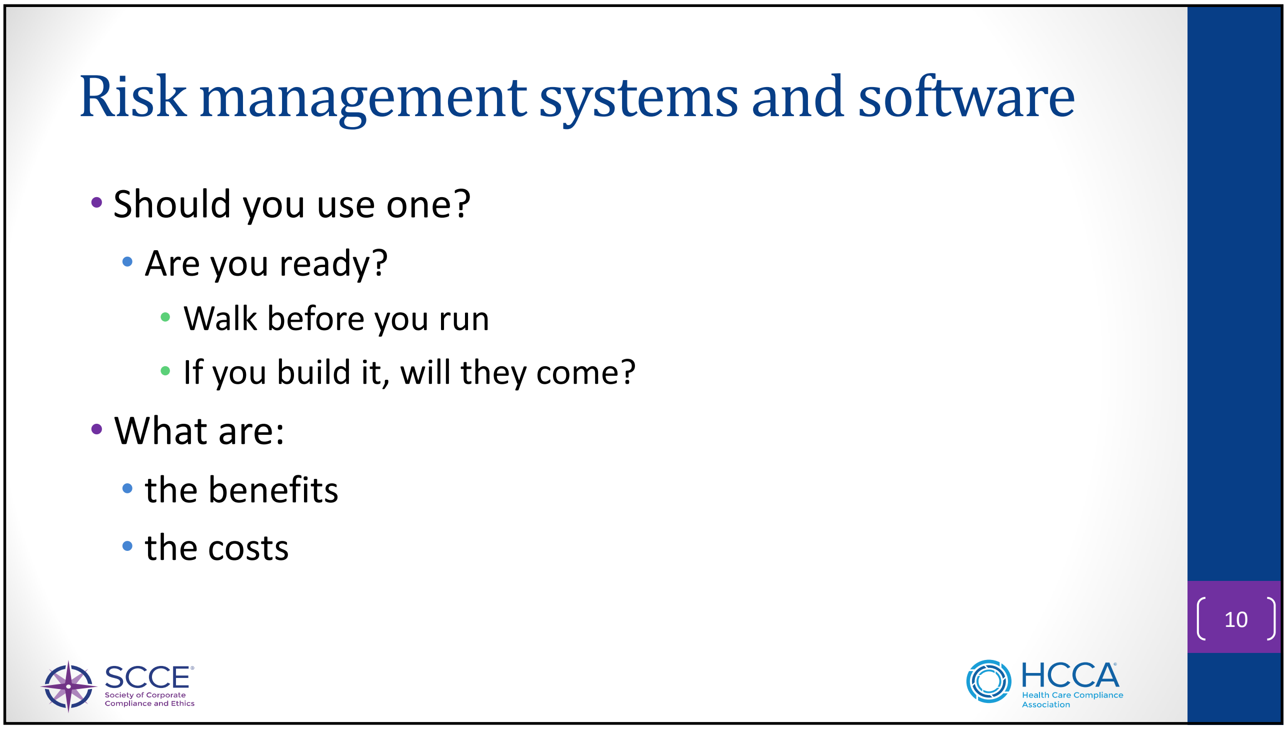
A. Psychological safety and sense of belonging
B. Organizational justice
C. “Speak-Up” culture
D. Diversity of opinions and perspectives
E. Values-based company mission
F. All of the above

9

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

9



Risk management systems and software

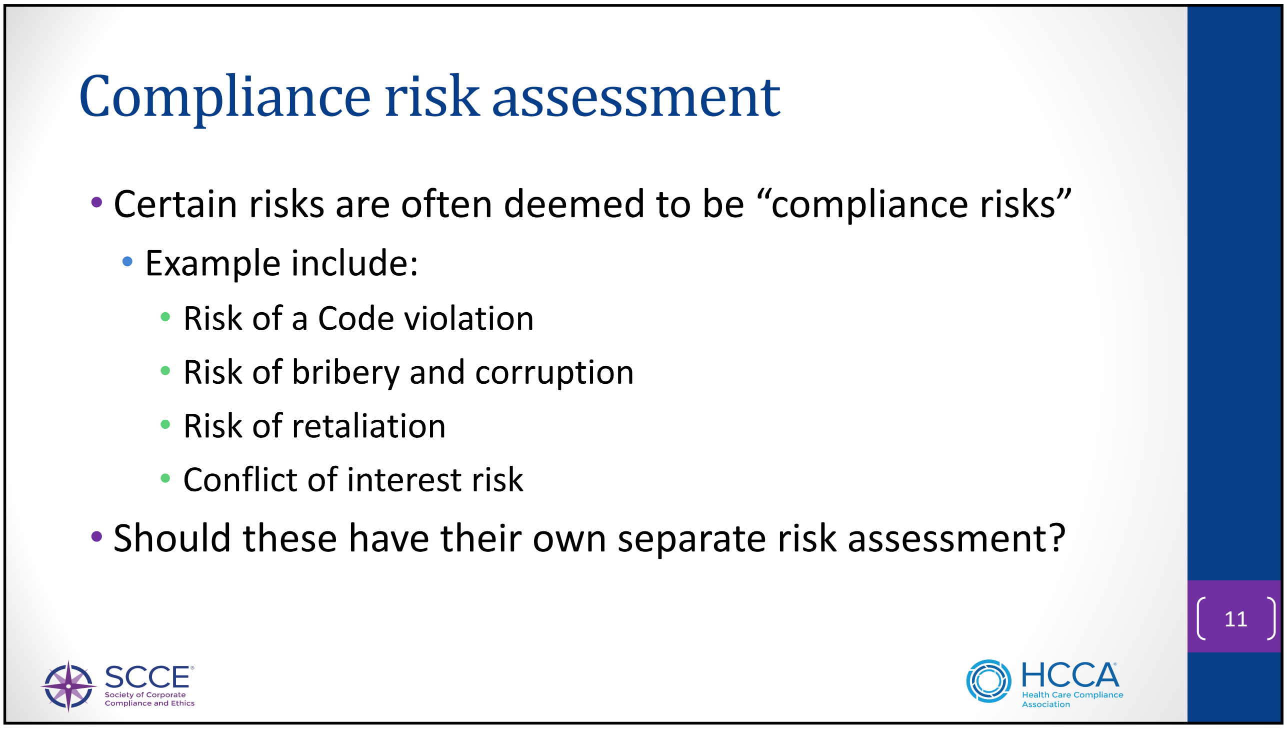
- Should you use one?
  - Are you ready?
    - Walk before you run
    - If you build it, will they come?
- What are:
  - the benefits
  - the costs

10

SCCE Society of Corporate Compliance and Ethics

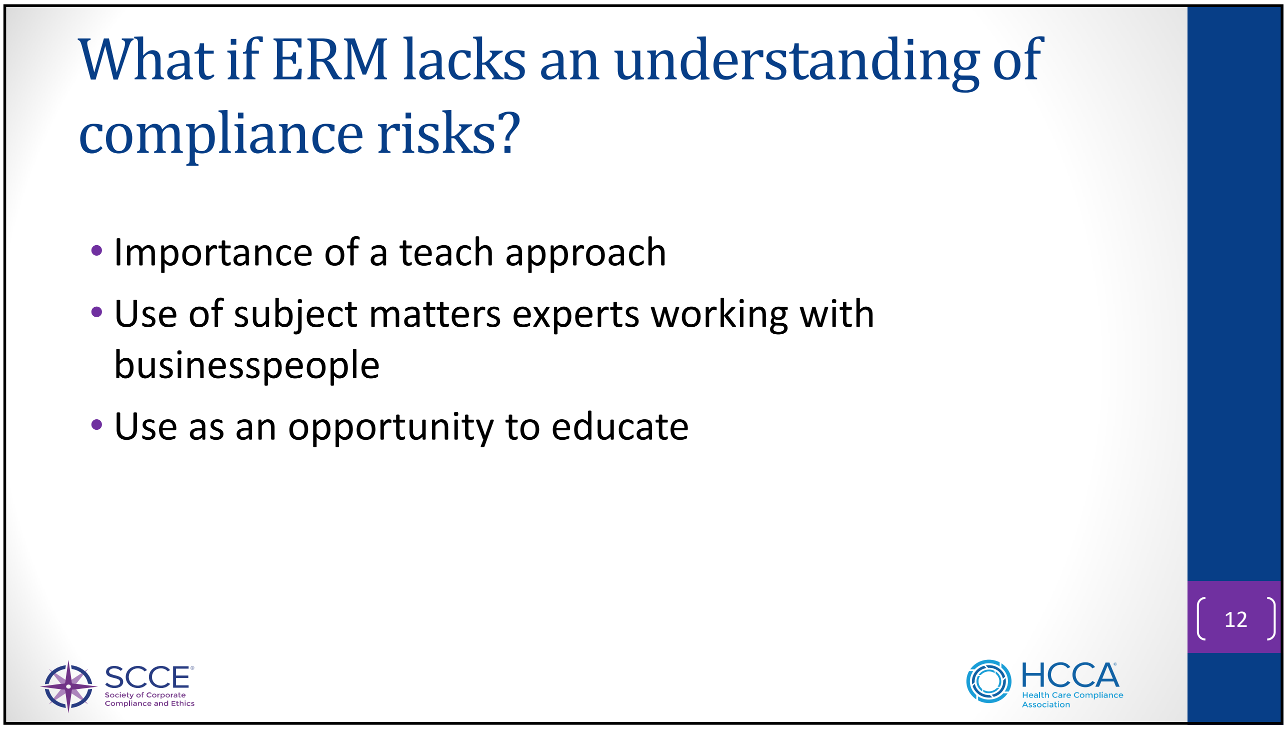
HCCA Health Care Compliance Association

10



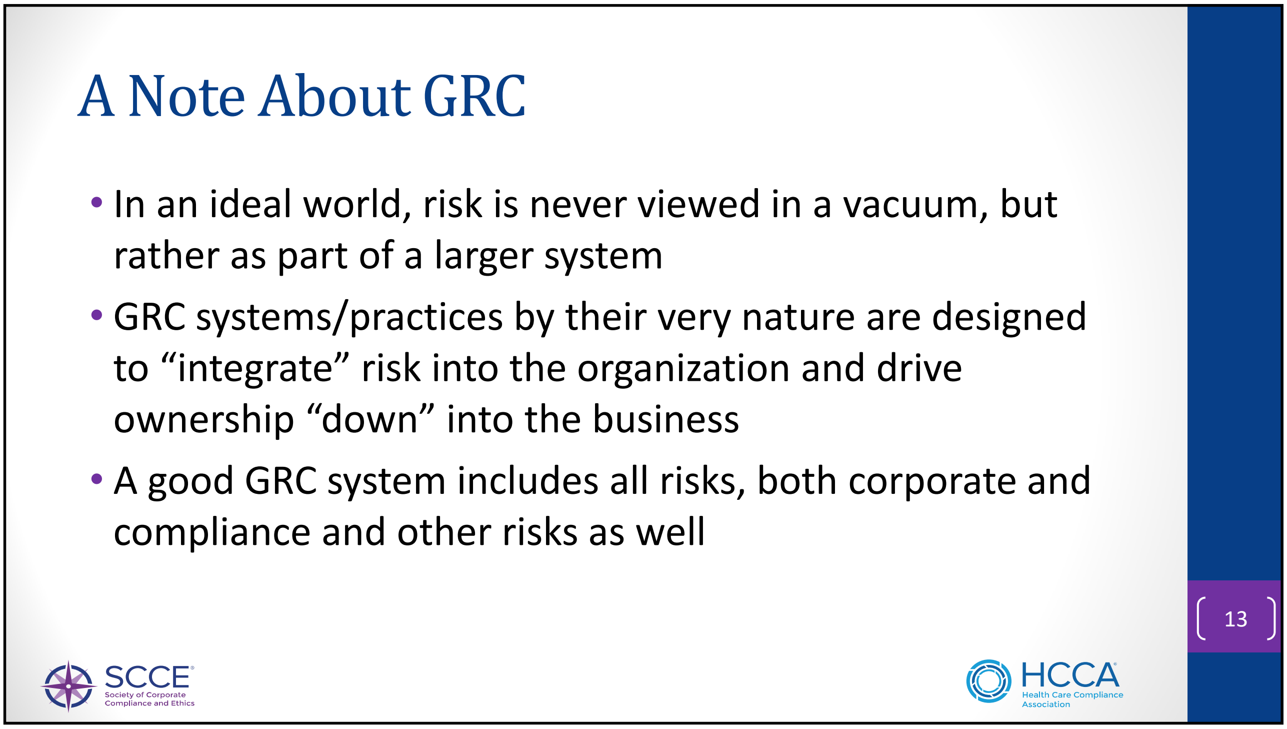
Compliance risk assessment

- Certain risks are often deemed to be “compliance risks”
  - Example include:
    - Risk of a Code violation
    - Risk of bribery and corruption
    - Risk of retaliation
    - Conflict of interest risk
- Should these have their own separate risk assessment?



What if ERM lacks an understanding of compliance risks?

- Importance of a teach approach
- Use of subject matters experts working with businesspeople
- Use as an opportunity to educate

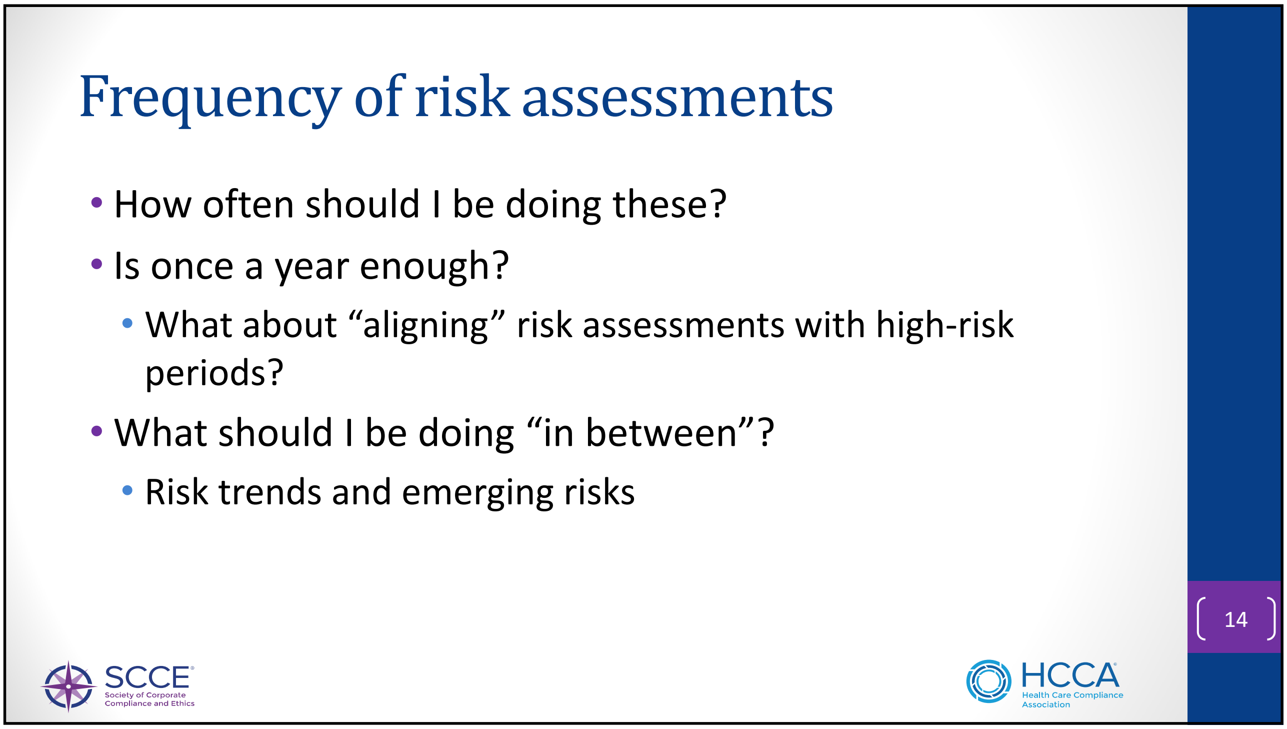


A Note About GRC

- In an ideal world, risk is never viewed in a vacuum, but rather as part of a larger system
- GRC systems/practices by their very nature are designed to “integrate” risk into the organization and drive ownership “down” into the business
- A good GRC system includes all risks, both corporate and compliance and other risks as well

13

13

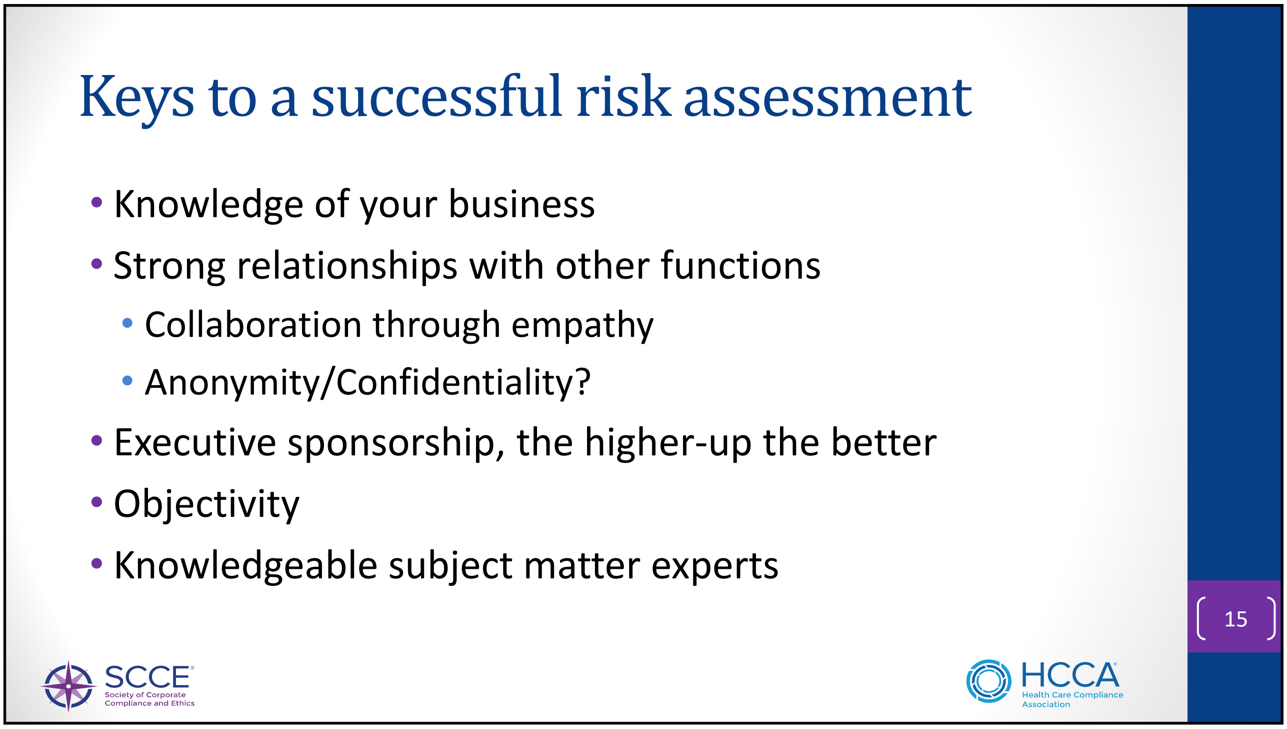


Frequency of risk assessments

- How often should I be doing these?
- Is once a year enough?
  - What about “aligning” risk assessments with high-risk periods?
- What should I be doing “in between”?
  - Risk trends and emerging risks

14

14

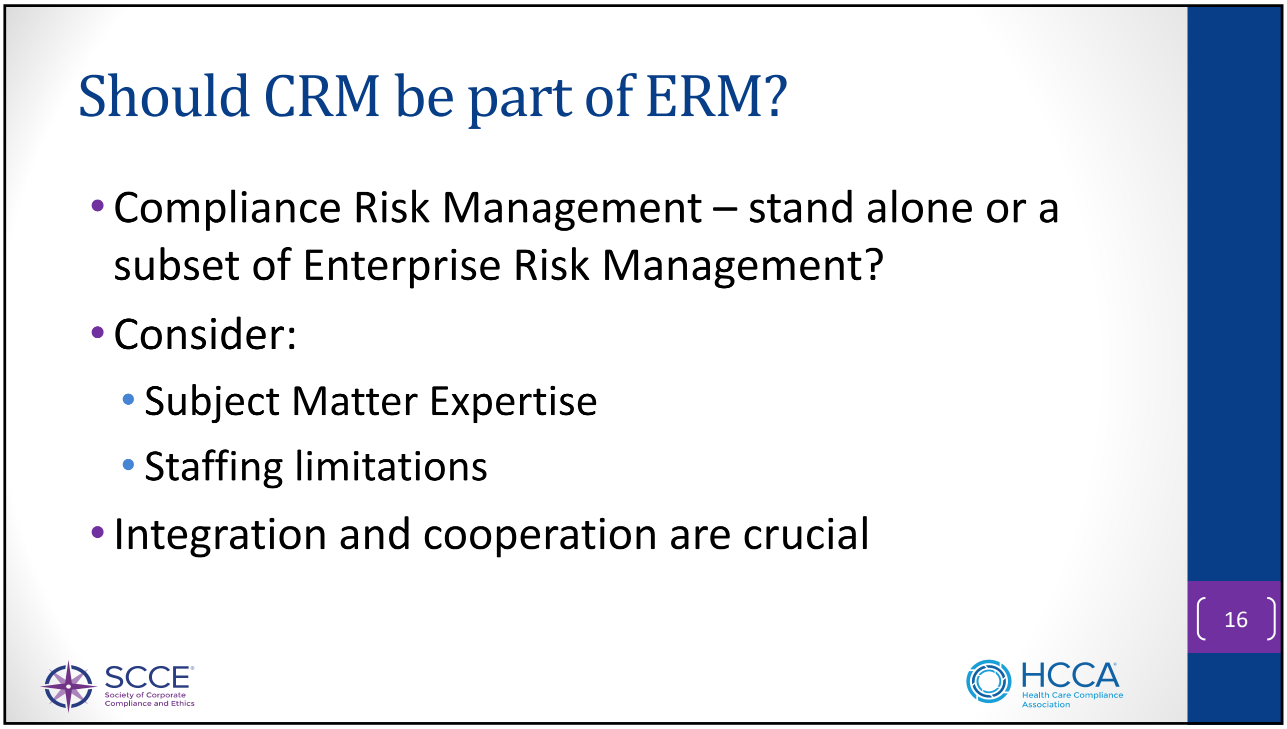


Keys to a successful risk assessment

- Knowledge of your business
- Strong relationships with other functions
  - Collaboration through empathy
  - Anonymity/Confidentiality?
- Executive sponsorship, the higher-up the better
- Objectivity
- Knowledgeable subject matter experts

15

15

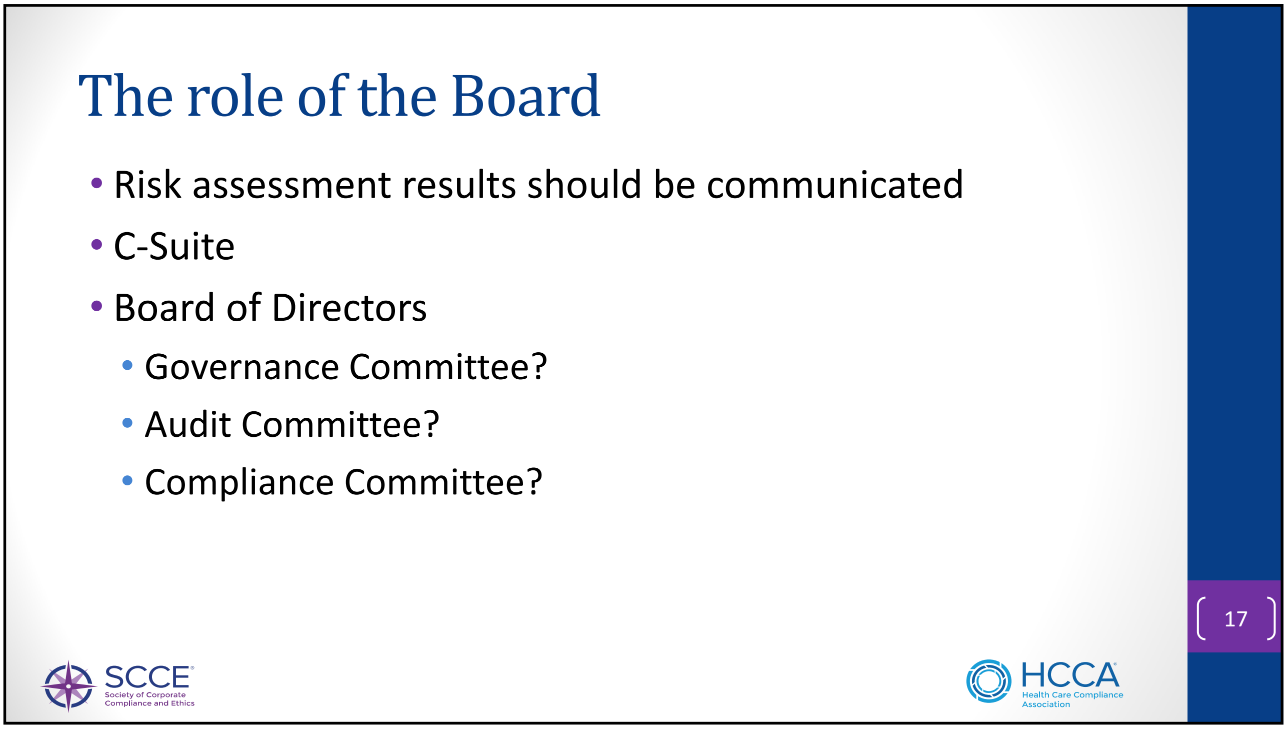


Should CRM be part of ERM?

- Compliance Risk Management – stand alone or a subset of Enterprise Risk Management?
- Consider:
  - Subject Matter Expertise
  - Staffing limitations
- Integration and cooperation are crucial

16

16



The role of the Board

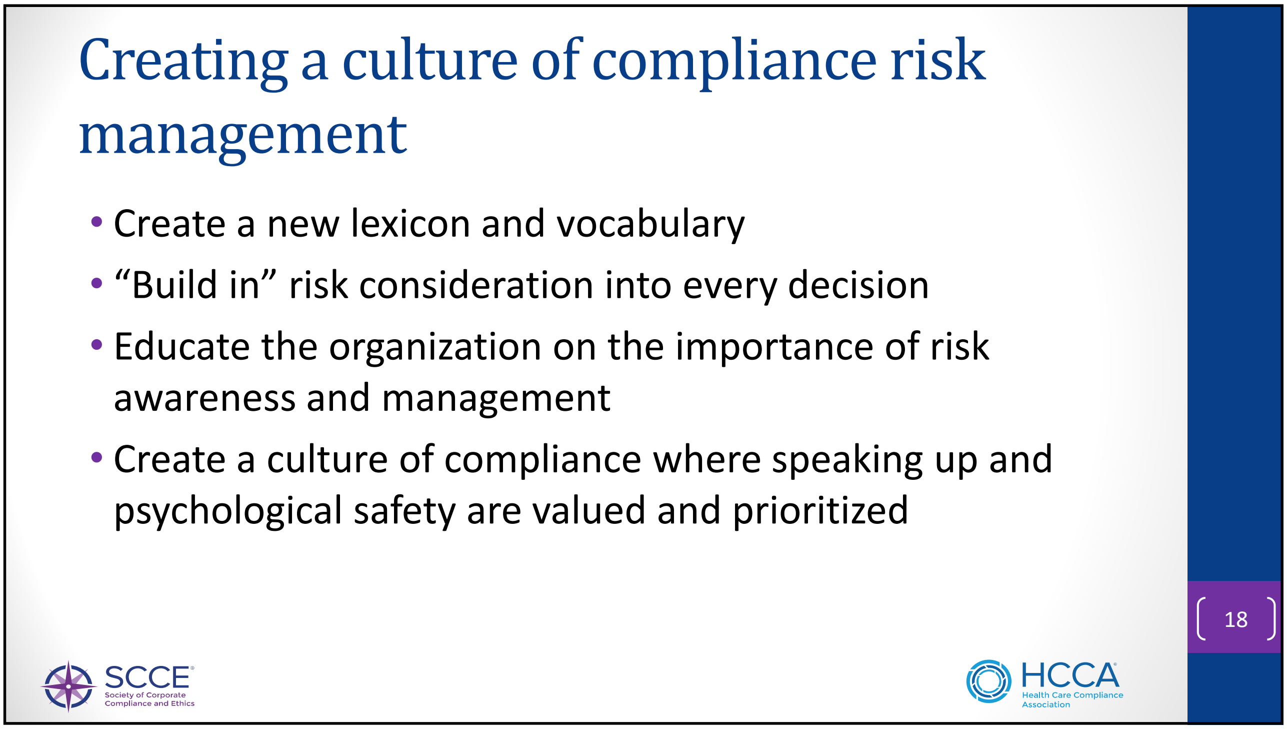
- Risk assessment results should be communicated
- C-Suite
- Board of Directors
  - Governance Committee?
  - Audit Committee?
  - Compliance Committee?

17

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

17



Creating a culture of compliance risk management

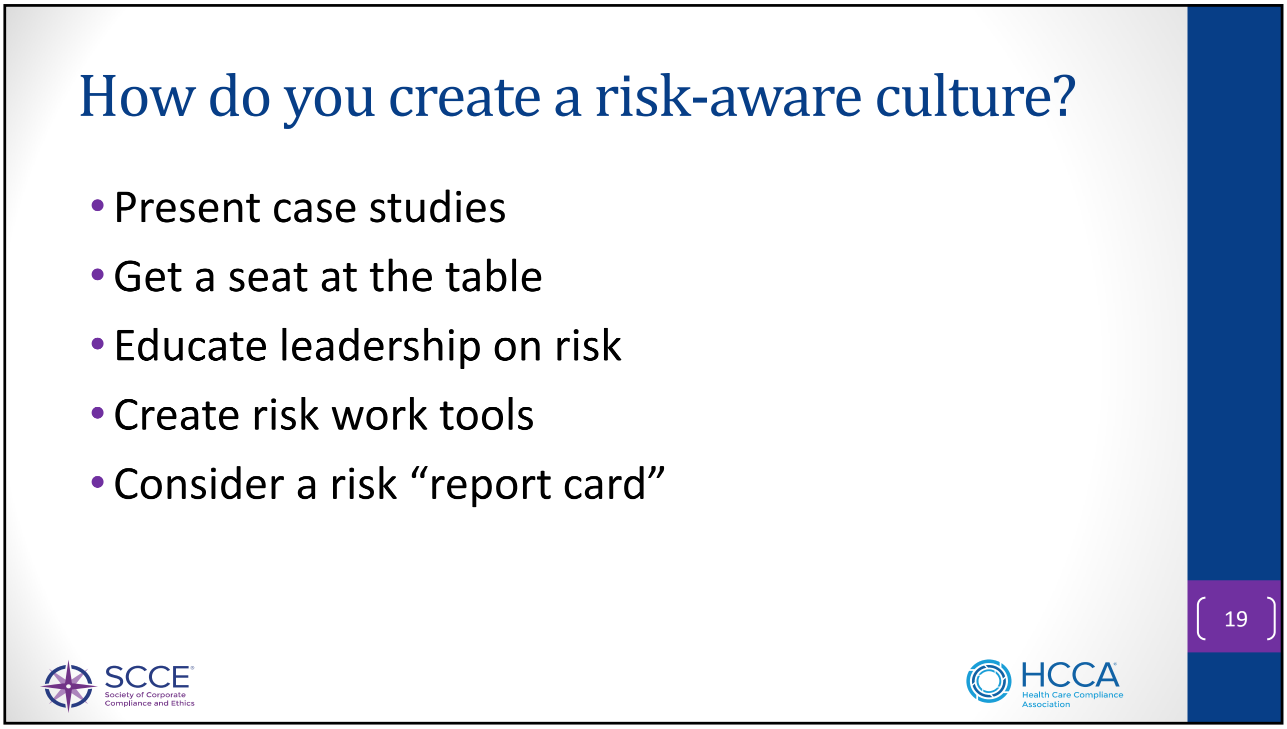
- Create a new lexicon and vocabulary
- “Build in” risk consideration into every decision
- Educate the organization on the importance of risk awareness and management
- Create a culture of compliance where speaking up and psychological safety are valued and prioritized

18

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

18

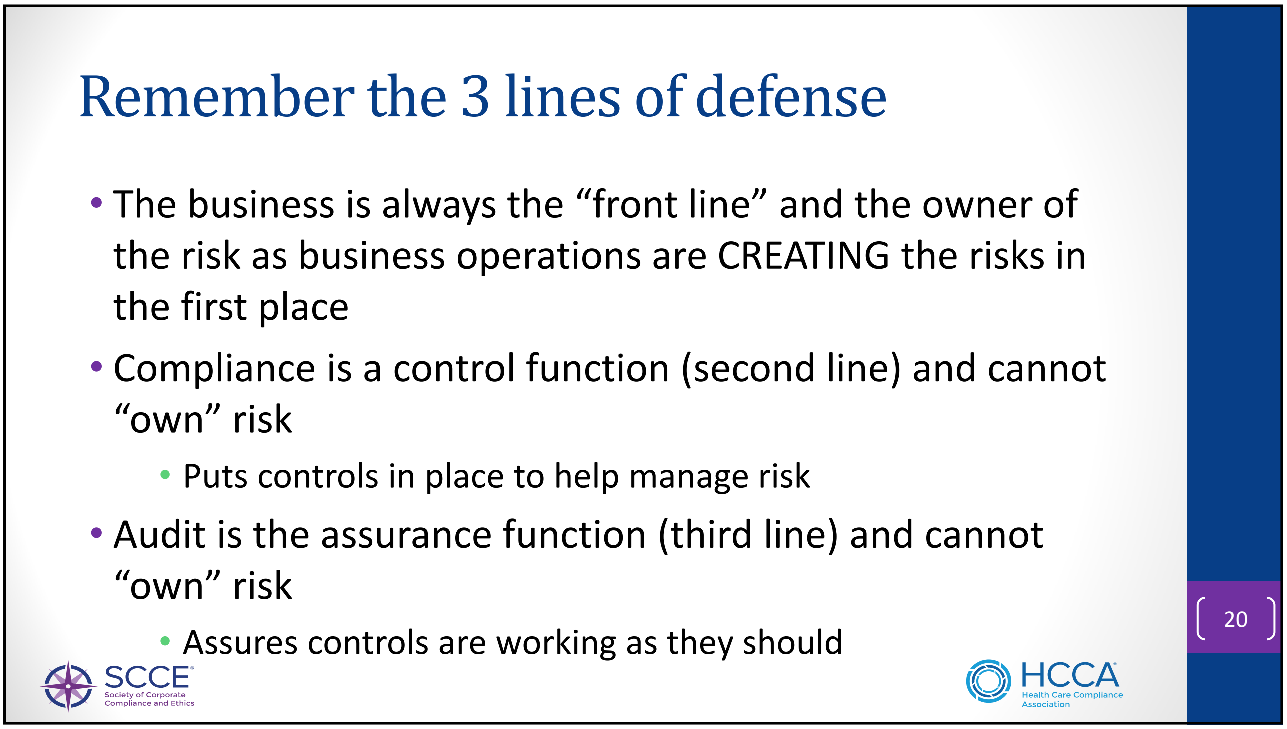


How do you create a risk-aware culture?

- Present case studies
- Get a seat at the table
- Educate leadership on risk
- Create risk work tools
- Consider a risk “report card”

19

19

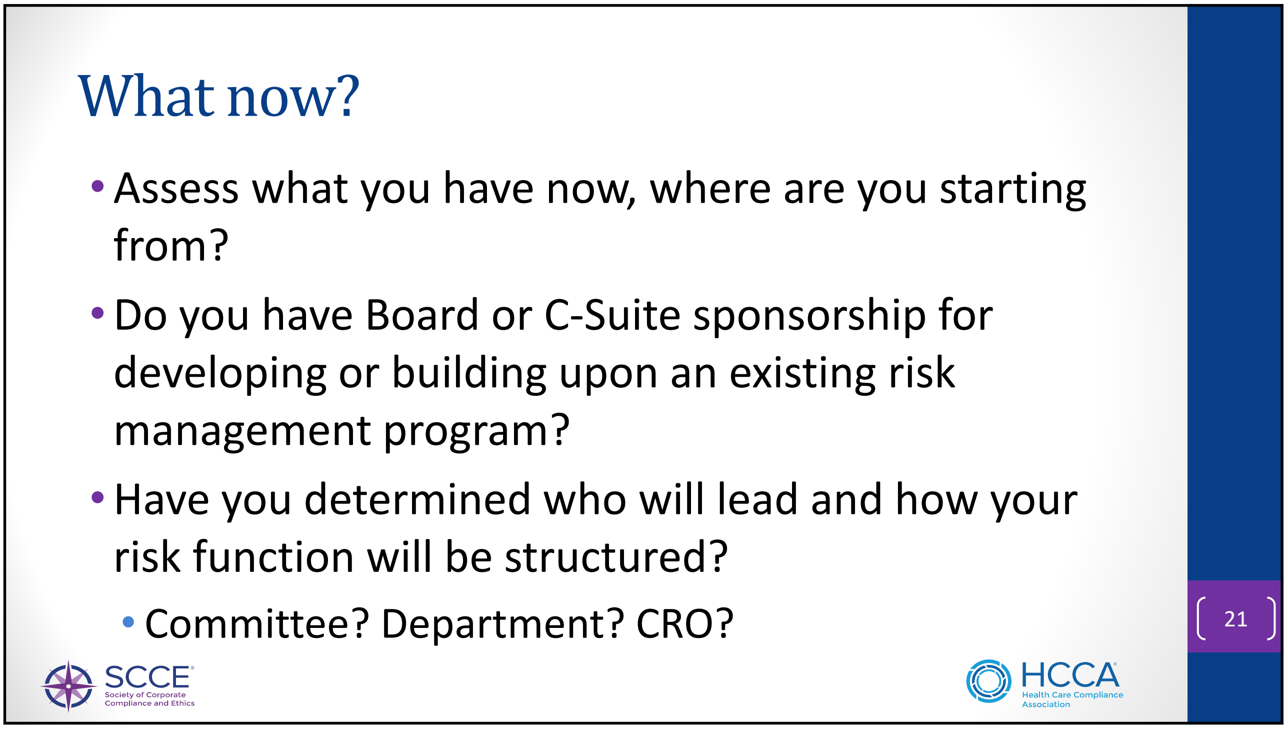


Remember the 3 lines of defense

- The business is always the “front line” and the owner of the risk as business operations are CREATING the risks in the first place
- Compliance is a control function (second line) and cannot “own” risk
  - Puts controls in place to help manage risk
- Audit is the assurance function (third line) and cannot “own” risk
  - Assures controls are working as they should

20

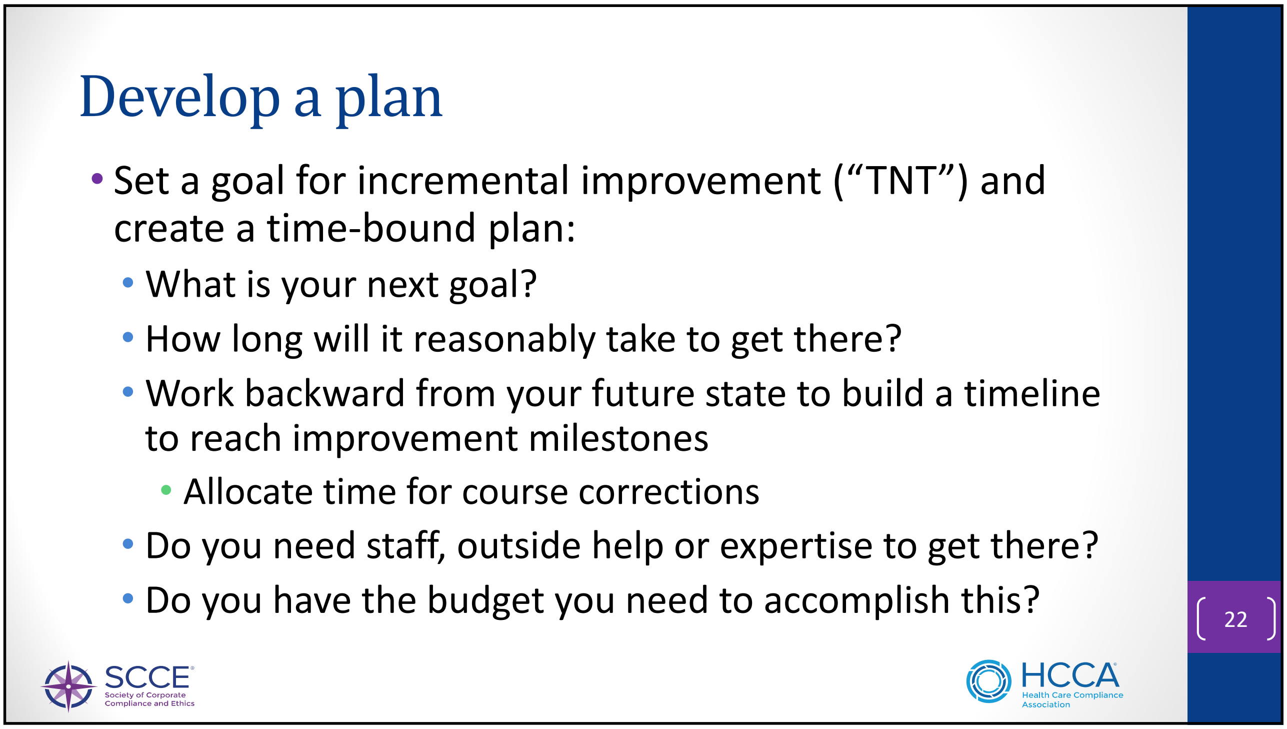
20



What now?

- Assess what you have now, where are you starting from?
- Do you have Board or C-Suite sponsorship for developing or building upon an existing risk management program?
- Have you determined who will lead and how your risk function will be structured?
  - Committee? Department? CRO?

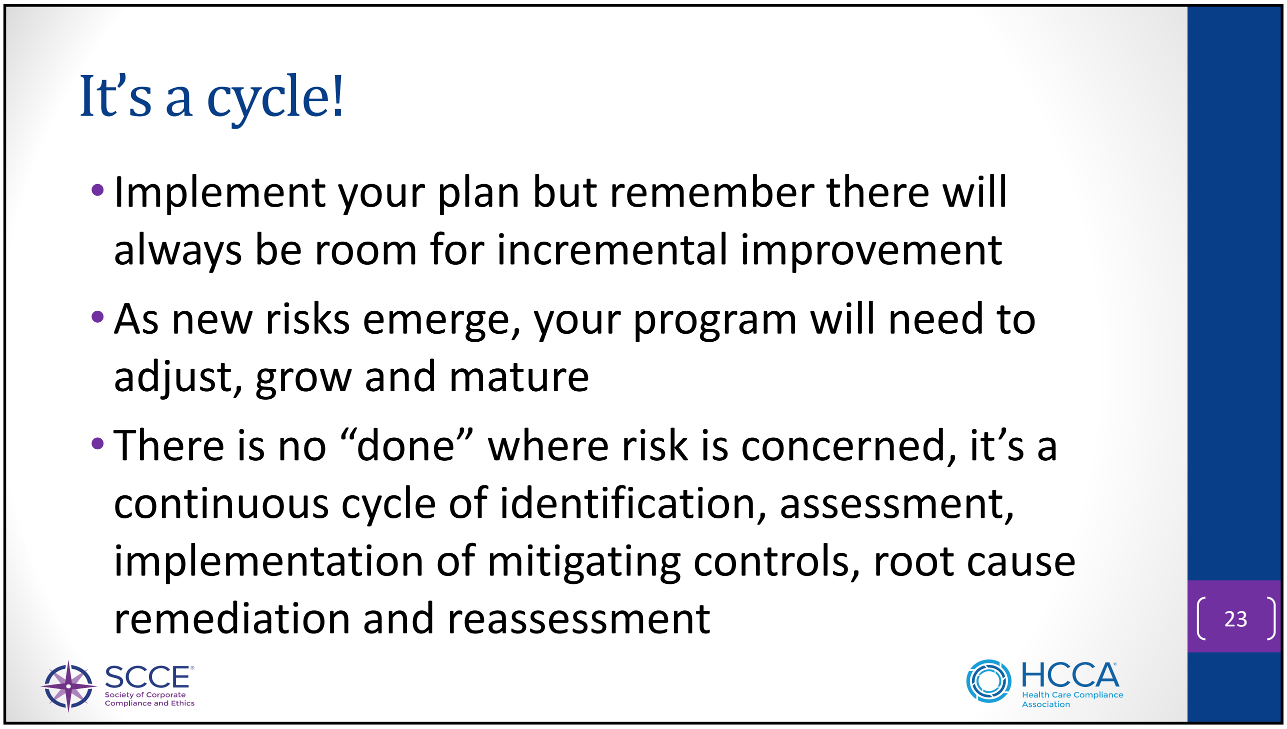
21



Develop a plan

- Set a goal for incremental improvement (“TNT”) and create a time-bound plan:
  - What is your next goal?
  - How long will it reasonably take to get there?
  - Work backward from your future state to build a timeline to reach improvement milestones
    - Allocate time for course corrections
  - Do you need staff, outside help or expertise to get there?
  - Do you have the budget you need to accomplish this?

22



It’s a cycle!

- Implement your plan but remember there will always be room for incremental improvement
- As new risks emerge, your program will need to adjust, grow and mature
- There is no “done” where risk is concerned, it’s a continuous cycle of identification, assessment, implementation of mitigating controls, root cause remediation and reassessment