



1

Judith W. Spain J.D., CCEP

President,
Higher Education Compliance Consulting

Professor Emeritus,
Eastern Kentucky University

Compliance Collaborative Program Consultant,
Georgia Independent College Association



Welcome.



Higher
Education
Compliance
Consulting



GEORGIA INDEPENDENT
COLLEGE ASSOCIATION

2

“

‘Workaholics aren’t heroes.

They don’t save the day; they use it up.

The real hero is already home... Because she figured
out a faster way to get things done.”

Jason Fried & David Heinemeire Hansson

Happyologist.co.uk

3

Agenda

Overview

Federal Sentencing Guidelines

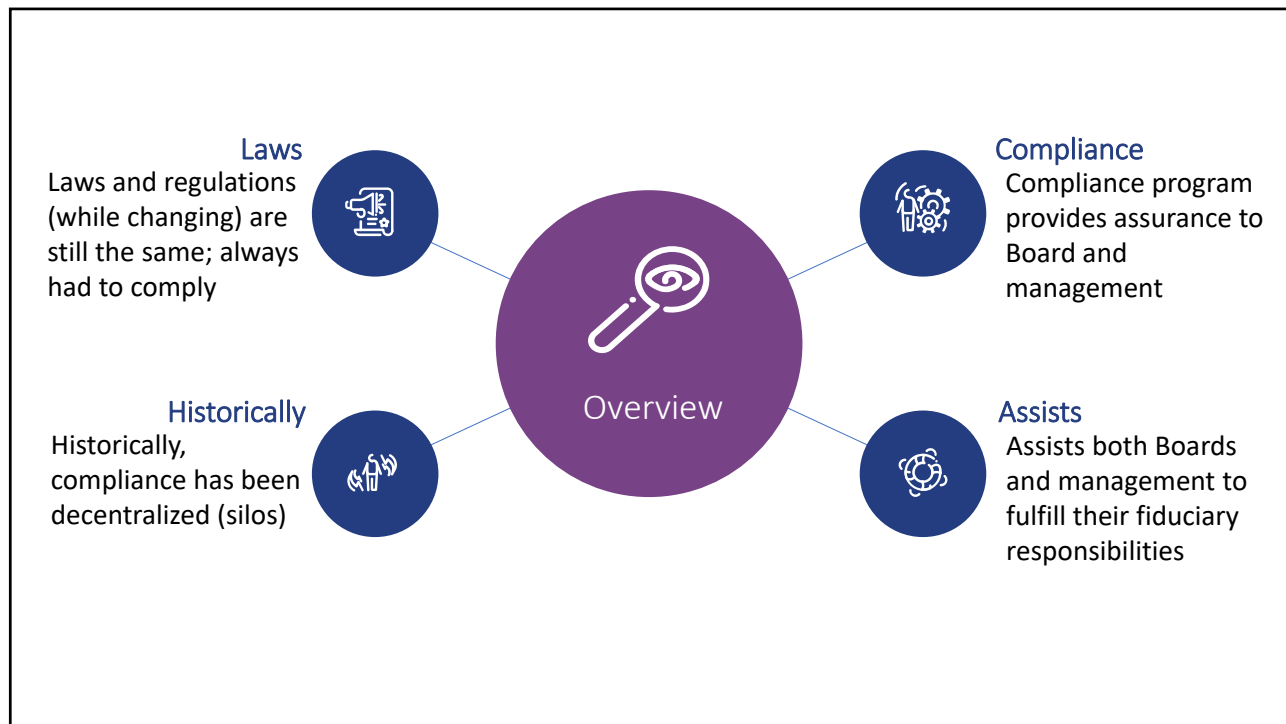
Enterprise Risk Management or Compliance Risk Assessment

Develop Compliance Risk Mitigation Plan

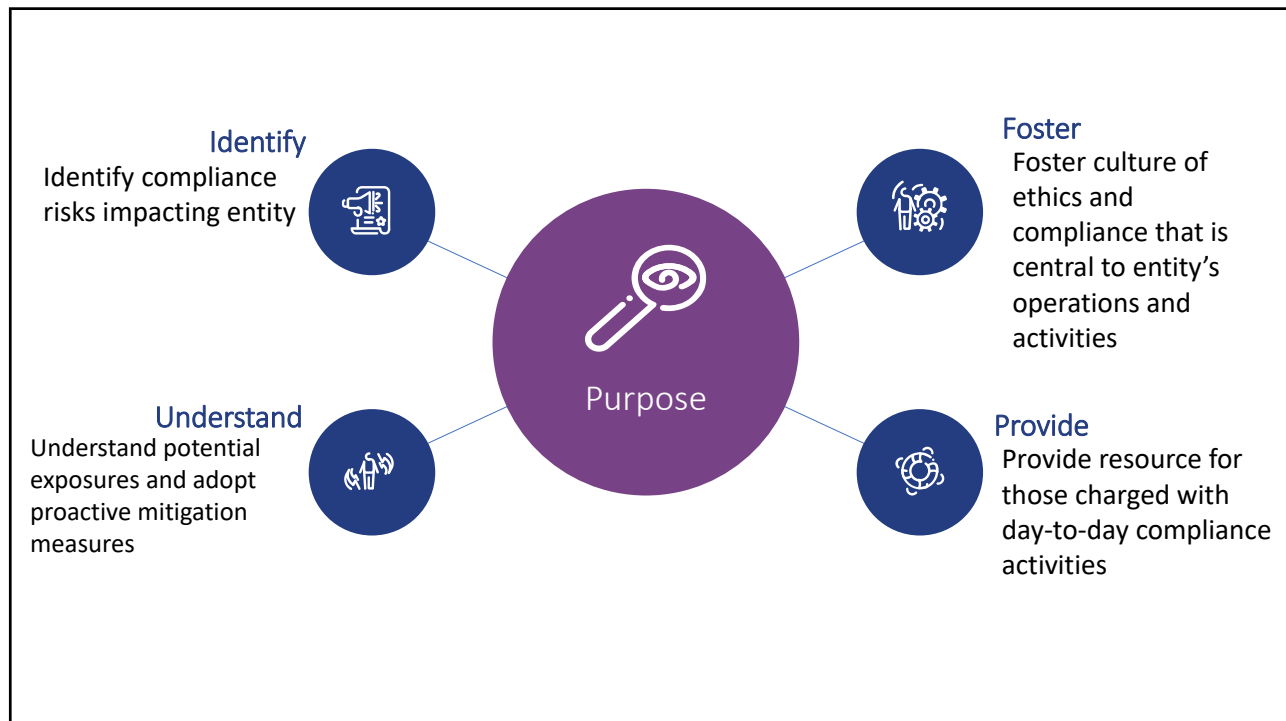
Examples

Action Items

4



5

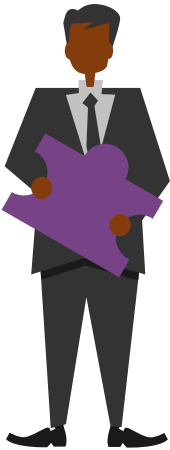


6




7

Compliance Program



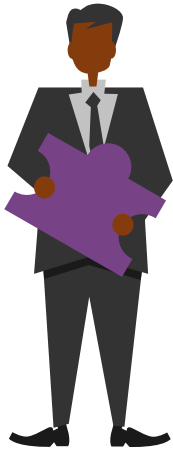
To have an effective compliance program, an organization must establish and maintain an organizational culture that “encourages ethical conduct and a commitment to compliance with the law.”

U.S. Federal Sentencing Guidelines §8B2.1(a)(2)



8

Federal Sentencing Guidelines Elements



1. High level personnel who exercise effective oversight and have direct reporting authority to the governing body;
2. Hiring practices;
3. Standards and procedures to prevent and detect criminal conduct;
4. Lines of communication;
5. Internal compliance monitoring;
6. Well-publicized disciplinary guidelines;
7. Response to detected offenses.



9



**Enterprise Risk Management or
Compliance Risk Management**

10

Enterprise Risk Management

Holistic approach

Considers possible risks to entity, employees, shareholders, and (perhaps) society

Process requires more than assessing and addressing risk

ERM framework looks at risk management in context of:

- Governance and culture
- Business strategy and objective-setting
- Performance
- Review and revision
- Information, communication, and reporting

11

Compliance Risk Management

Slice of ERM

Identifies legal and regulatory risks

Evaluates if organization is complying with law/regulation

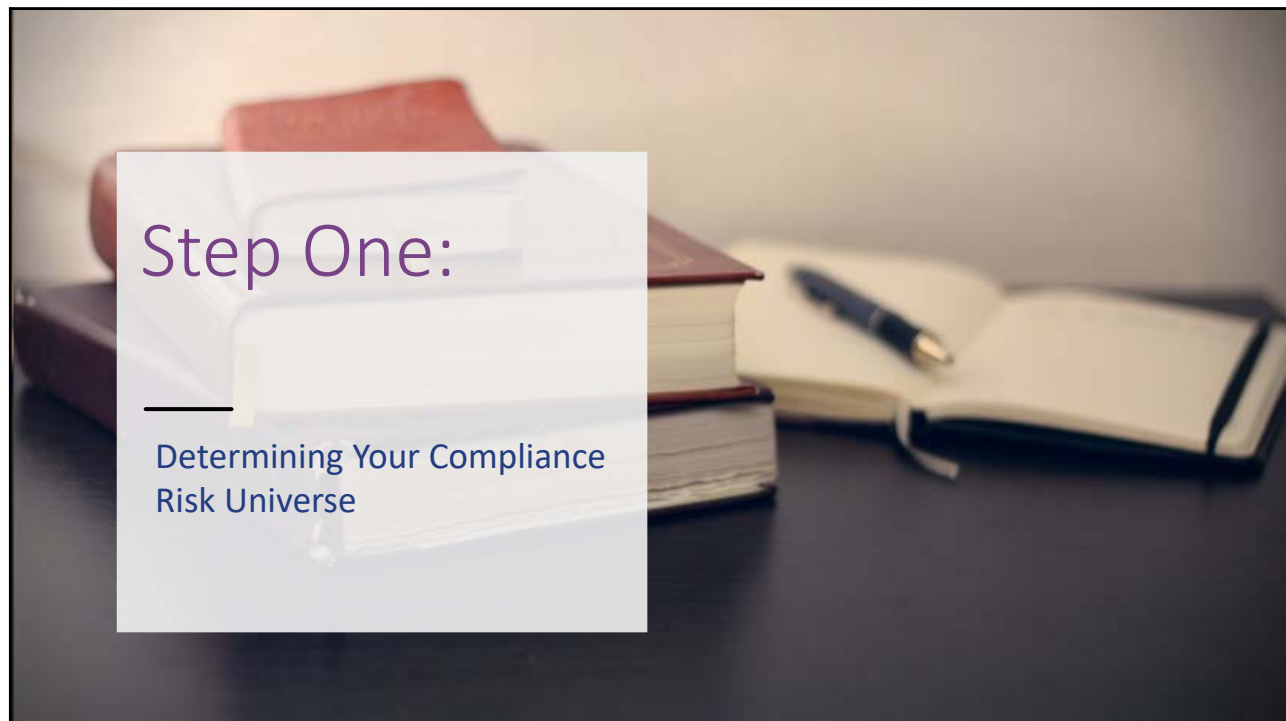
Maximizes use of limited resources by directing resources to most significant compliance issues

Develops a mitigation plan to focus on compliance with law/regulation

12



13



14

Compliance Risk Identification



What are the possible compliance risks your entity faces?



What issues keep you up at night?



Utilizing existing registries with customization for your entity?

15

Option 1 – Adopt risk universe used by similarly situated businesses



Use predetermined lists of applicable laws and/or regulations from nationally recognized organizations;



Exercise due diligence by various administrators to identify other applicable laws and/or regulations



16

Option 2 – Conduct interviews of key employees



Interviews determine which laws and regulations that key administrators deal with every day/month/year



Caution:

- Administrators being interviewed may, or may not, know what they do not know
- Due diligence research to identify applicable laws and regulations
- Follow-up interviews when risk mitigation plan takes shape



17

Step Two:

Determining Likelihood
Of Occurrence



18

Definition – Likelihood of Occurrence



Probability that noncompliance with a law or regulation will occur daily, monthly, yearly, once every five years, once every 10 years, etc.



Uses two factors to determine potential for encountering risk

- Existing controls
- Frequency of noncompliance



19

Likelihood of Occurrence Factors			
Rank/Scale		Measure of Likelihood	
		Existing Controls	Frequency of Noncompliance
1	Rare	<ul style="list-style-type: none"> • Policies mandated and updated regularly. • Regular mandatory training is provided to the identified responsible person(s) and is documented. • Regular management monitoring reviews are performed and documented. 	May only occur in exceptional circumstances Less than once in 10 years
2	Unlikely	<ul style="list-style-type: none"> • Policies mandated and updated regularly. • Regular training is provided to the identified responsible person(s), but not documented. • Regular management monitoring reviews are performed, but not documented. 	Could occur at some time At least once in 10 years
3	Possible	<ul style="list-style-type: none"> • Policies mandated, but not updated regularly. • Responsible person(s) identified. • Training is provided when needed. • Some management monitoring reviews are performed, but not documented. 	Might occur at some time At least once in 5 years
4	Likely	<ul style="list-style-type: none"> • Policies and procedures in place but neither mandated nor updated regularly. • Responsible person(s) identified. • Some formal and informal (on the job) training. • No management monitoring reviews. 	Will probably occur At least once per year
5	Almost Certain	<ul style="list-style-type: none"> • No controls in place. • No policies or procedures, no responsible person(s) identified, no training, and no management monitoring reviews. 	Expected to occur in most circumstances More than once per year

20

How to Evaluate Factors



- Chose 1 through 5 for BOTH factors of likelihood of noncompliance
 - “Existing Controls” and “Frequency of Noncompliance”



Existing controls and frequency of noncompliance

- Both dependent and independent factors
 - Dependent
 - If no controls in place, noncompliance will occur more frequently
 - Independent
 - Even if controls in place, the number of times a law must be complied with increases the likelihood of a single instance or multiple instances of noncompliance



21

Action Items



- Identify and define what measures of likelihood of occurrence factors to use



- Agree on numerical scale (1-3, 1-5, ?) and/or word choice scale



- Work closely with IT before beginning assessment process to determine best method for data displayed in risk mitigation plan



22



23

Definition – Impact of Occurrence

Probability that noncompliant incident will have a measurably negative effect on the business



- Financial resources being depleted
- Damage to business reputation
- Destruction of vital documents due to a security breach
- Other potential harm to the organization



24

Impact of Occurrence Factors								
Rank/Scale		Measure of Impact						
		Legal/ Compliance	Health and Safety	Financial Monetary	Assets	Strategic	Potential Disruption of Business Operations	Reputation and Image
1	Insignificant	In compliance	No injuries	TBD dollar amount or percentage of budget	Little or no impact	Little or no impact	< ½ day	Unsubstantiated, low impact, low profile or no news items
2	Minor	Civil violation with little/no fines	First aid treatment	TBD dollar amount or percentage of budget	Minor loss or damage	Minor impact	< 1 day	Substantiated, low impact, low news profile
3	Serious	Significant civil fines/penalties	Medical treatment	TBD dollar amount or percentage of budget	Major damage	Major impact	1 day-1 week	Substantiated, public embarrassment, moderate impact, moderate news profile
4	Disastrous	Serious violation, criminal prosecution probable	Death or extensive injuries	TBD dollar amount or percentage of budget	Significant loss	Significant impact	1 week-1 month	Substantiated, public embarrassment, high impact, high news profile, third party actions
5	Catastrophic	Significant violation, criminal conviction probable, loss of accreditation or licensure	Multiple deaths or several permanent disabilities	TBD dollar amount or percentage of budget	Complete loss of assets	Loss of accreditation or license	> 1 month	Substantiated, public embarrassment, very high multiple impacts, high widespread news profile, third party actions

25

How to Evaluate Factors



Choose 1 through 5 for each factor



No set number of factors used to determine impact of noncompliance



Customization is critical



Consider first assessment to include only some factors



Expand assessment to other factors once compliance initiative passes initial stages



26

Action Items



Identify and define what impact of occurrence factors to use



Agree on numerical scale (1-3, 1-5, ?) and/or word choice scale



Work closely with IT before beginning assessment process to determine best method for data displayed in risk mitigation plan



27

Step Four:

Conducting Compliance
Risk Assessment



28

Who Does the Work?

Legal

Executive Compliance Committee

Compliance Officer

Compliance Department

Compliance Partner



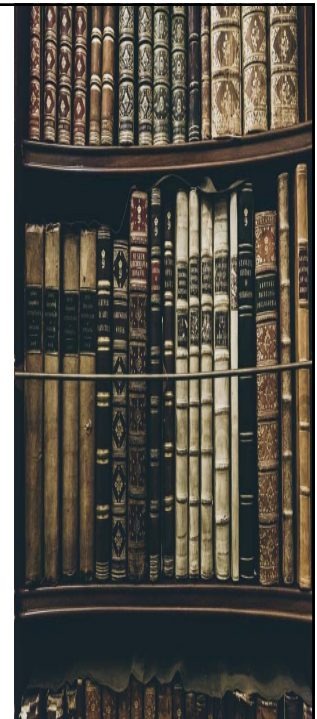
29

Survey Instrument – Part I

Identifies present controls in place to ensure compliance with a law or regulation

Identifies:

- Present policies, training, procedures, etc.
- How data is collected
- If physical inspection is required
- If required to send disclosure/report to outside agency
- Other industry specific controls



30

Survey Instrument – Part II

Identifies potential new or updated controls that could be put in place to ensure compliance with a law or regulation

Identifies what is missing in terms of

- Policies, training, procedures, etc.
- How data should be collected
- Whether physical inspection is required
- If sending disclosure/report to outside agency is required
- Other industry specific concerns

Not just employee's opinion

Response focuses on best practices, changes in laws, changes in training techniques, changes in industry standards, etc.



31

Survey Instrument – Part III

Open ended questions designed to identify additional concerns and/or compliance risks associated with a law or regulation

Identify any barriers or obstacles that might prevent or decrease compliance with the law or regulation

Be clear that requested responses are not to place blame



32

Action Items



Verify your compliance risk assessment will/will not be protected under attorney-client privilege or attorney-work product



Identify who completes survey



Design survey instrument



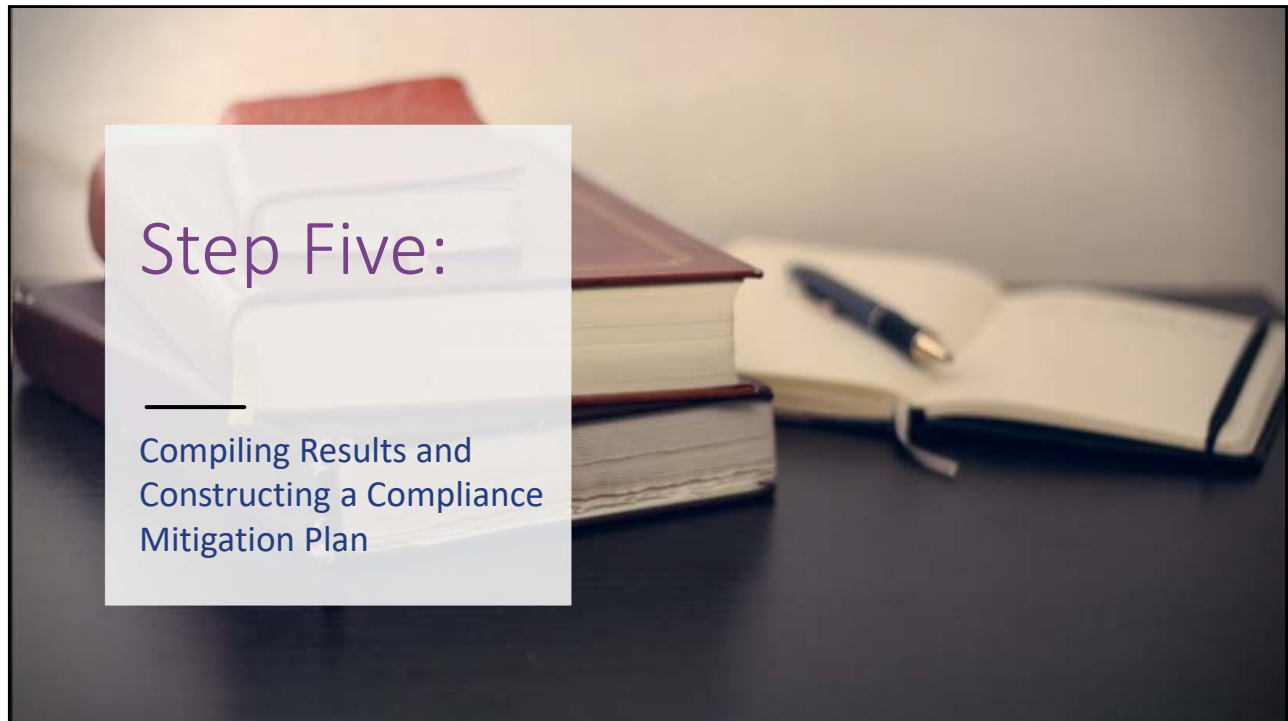
Plan mandatory training for any employee completing survey



33

Step Five:

Compiling Results and
Constructing a Compliance
Mitigation Plan



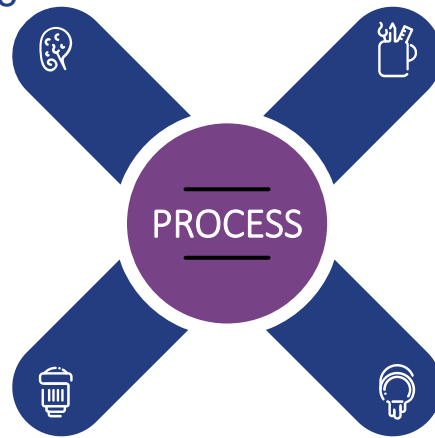
34



Review, Confirm Numbers, Compare

Consider preparing two matrixes; compare placement on heat map

Plot scores on heat map



Review survey responses

Confirm numerical scores for likelihood of occurrence and impact of occurrence

37

Prioritize Risk

Customize

High-risk focus, awareness of mid-level dangers, acknowledge the low-level risks



High-risk-only focus

All-risk focus

38





Mitigation Plan

- Rule details
- Summary
- Current state
- Costs versus occurrence likelihood
- Required changes
- Important changes



39

Action Items

-  Determine who generates compliance matrix
-  Determine how survey results are turned into numerical scores and plotted on matrix
-  Determine appetite for risk
-  Determine who prioritizes identified compliance risks to create risk mitigation plan




40



41

Monitor

- How to keep risk assessment process ongoing?
 - Develop and publicize compliance calendar
 - Perform random audits
 - Ensure employees have access to trainings to keep current
 - Review trends in employee discipline
 - Develop and implement a Reporting Policy



42

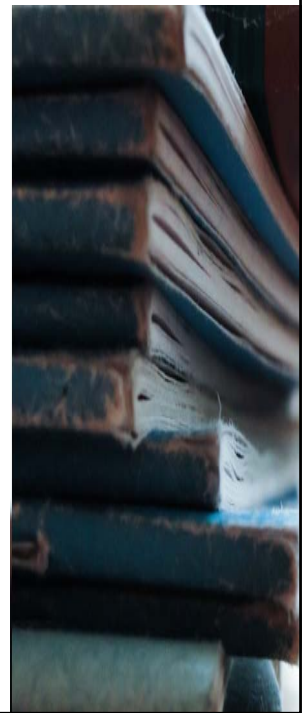
Reassess

Develop timetable for reassessing previously reviewed and assessed laws or regulations

Compile standardized templates for reassessment survey

Carefully review data-collection method to determine intersection of new analysis with previous analysis

- Show the dots on the matrix moving away from high impact/high likelihood quadrant to minimal impact/minimal likelihood quadrant



43

Modify

Identify trends

Conduct root-cause analysis

Implement ongoing modifications



44

Pick an Example



Family Medical Leave Act

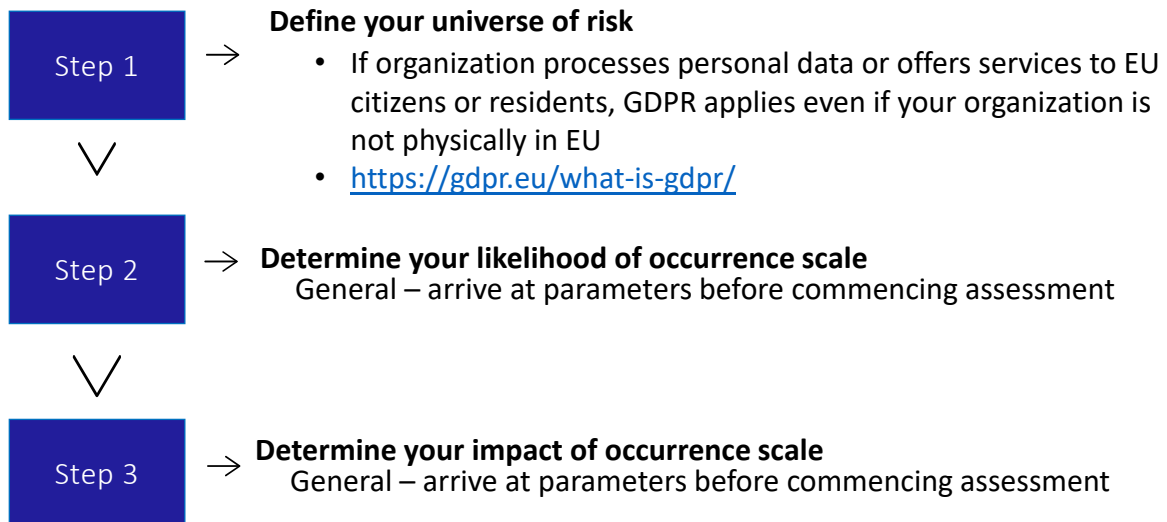
General Data Protection Regulations

Youth Protection Programs - Negligent Hiring

Title IX, Education Amendments of 1972

45

General Data Protection Regulation



46

GDPR – Assessment Process

Step 4



Conducting Compliance Risk Survey

- Part I – what does your organization have in place – policy, procedure, training, etc.?
- Part II – what should your organization have in place?
- Part III – what risks have not been identified that are unique to your organization?



Step 5



Develop Compliance Universe Matrix (Heat Map)

- What is likelihood of occurrence?
 - Specific
 - How many EU citizens or residents does your organization possess data for or offers services to these citizens/residents?
 - Arrive at a numerical score
- What is impact of occurrence?
 - Specific
 - Maximum of €20 million or 4% of global revenue (whichever is higher)
 - Data subjects have the right to seek compensation for damages.
 - Damage to reputation
 - No physical harm
 - Arrive at a numerical score

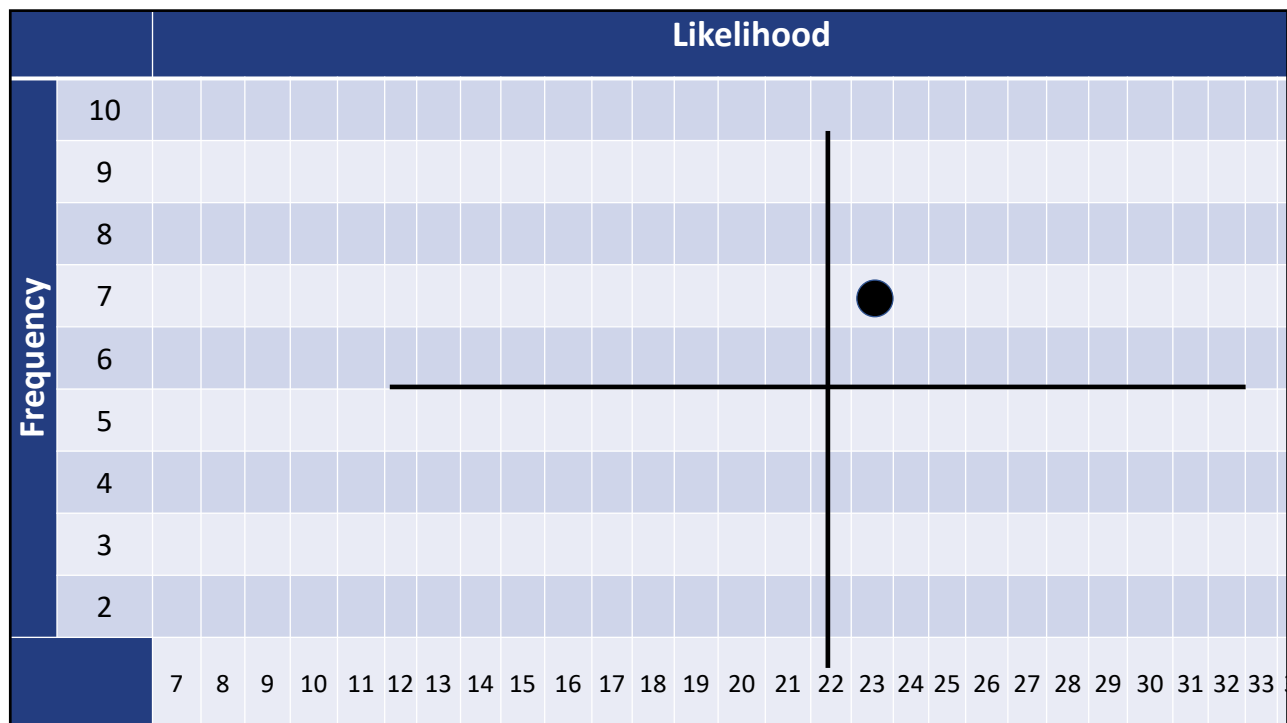
47

Likelihood of Occurrence Factors			
Rank/Scale		Measure of Likelihood	
		Existing Controls	Frequency of Noncompliance
1	Rare	<ul style="list-style-type: none"> • Policies mandated and updated regularly. • Regular mandatory training is provided to the identified responsible person(s) and is documented. • Regular management monitoring reviews are performed and documented. 	May only occur in exceptional circumstances Less than once in 10 years
2	Unlikely	<ul style="list-style-type: none"> • Policies mandated and updated regularly. • Regular training is provided to the identified responsible person(s), but not documented. • Regular management monitoring reviews are performed, but not documented. 	Could occur at some time At least once in 10 years
3	Possible	<ul style="list-style-type: none"> • Policies mandated, but not updated regularly. • Responsible person(s) identified. • Training is provided when needed. • Some management monitoring reviews are performed, but not documented. 	Might occur at some time At least once in 5 years
4	Likely	<ul style="list-style-type: none"> • Policies and procedures in place but neither mandated nor updated regularly. • Responsible person(s) identified. • Some formal and informal (on the job) training. • No management monitoring reviews. 	Will probably occur At least once per year
5	Almost Certain	<ul style="list-style-type: none"> • No controls in place. • No policies or procedures, no responsible person(s) identified, no training, and no management monitoring reviews. 	Expected to occur in most circumstances More than once per year

48

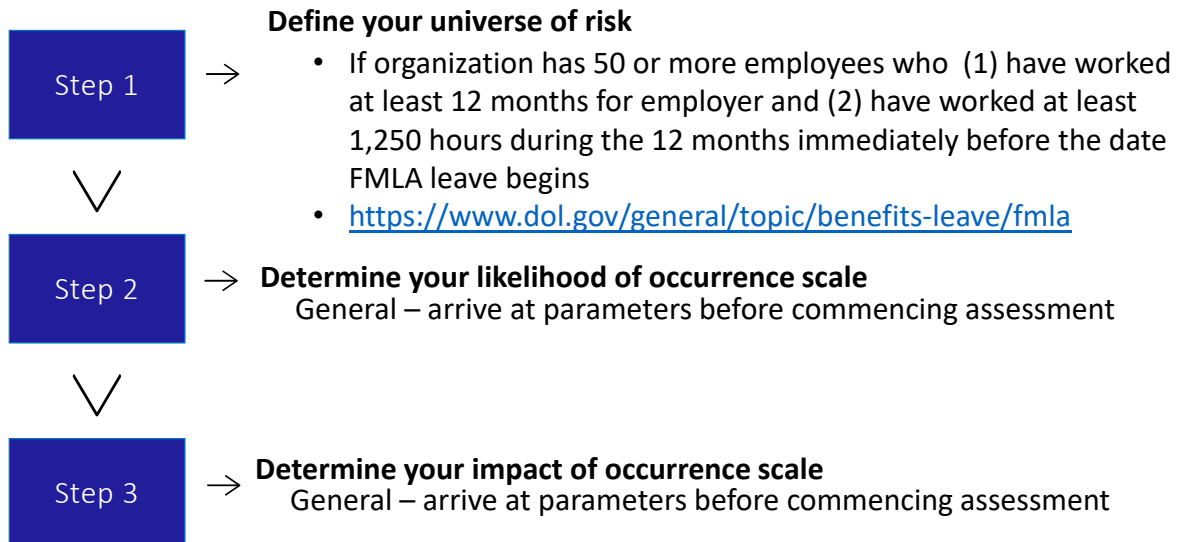
Impact of Occurrence Factors								
Rank/Scale		Measure of Impact						
		Legal/ Compliance	Health and Safety	Financial		Strategic	Potential Disruption of Business Operations	Reputation and Image
1	Insignificant	In compliance	No injuries	TBD dollar amount or percentage of budget	Little or no impact	Little or no impact	< ½ day	Unsubstantiated, low impact, low profile or no news items
2	Minor	Civil violation with little/no fines	First aid treatment	TBD dollar amount or percentage of budget	Minor loss or damage	Minor impact	< 1 day	Substantiated, low impact, low news profile
3	Serious	Significant civil fines/penalties	Medical treatment	TBD dollar amount or percentage of budget	Major damage	Major impact	1 day-1 week	Substantiated, public embarrassment, moderate impact, moderate news profile
4	Disastrous	Serious violation, criminal prosecution probable	Death or extensive injuries	TBD dollar amount or percentage of budget	Significant loss	Significant impact	1 week-1 month	Substantiated, public embarrassment, high impact, high news profile, third party actions
5	Catastrophic	Significant violation, criminal conviction probable, loss of accreditation or	Multiple deaths or several permanent disabilities	TBD dollar amount or percentage of budget	Complete loss of assets	Loss of accreditation or license	> 1 month	Substantiated, public embarrassment, very high multiple impacts, high widespread news profile, third party

49



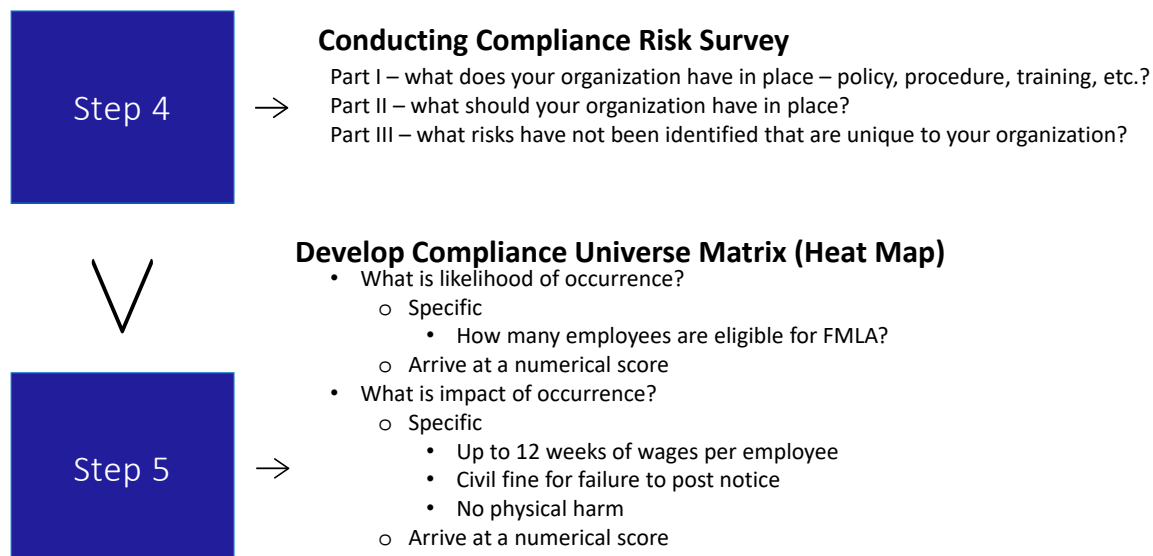
50

Family Medical Leave Act



51

FMLA – Assessment Process



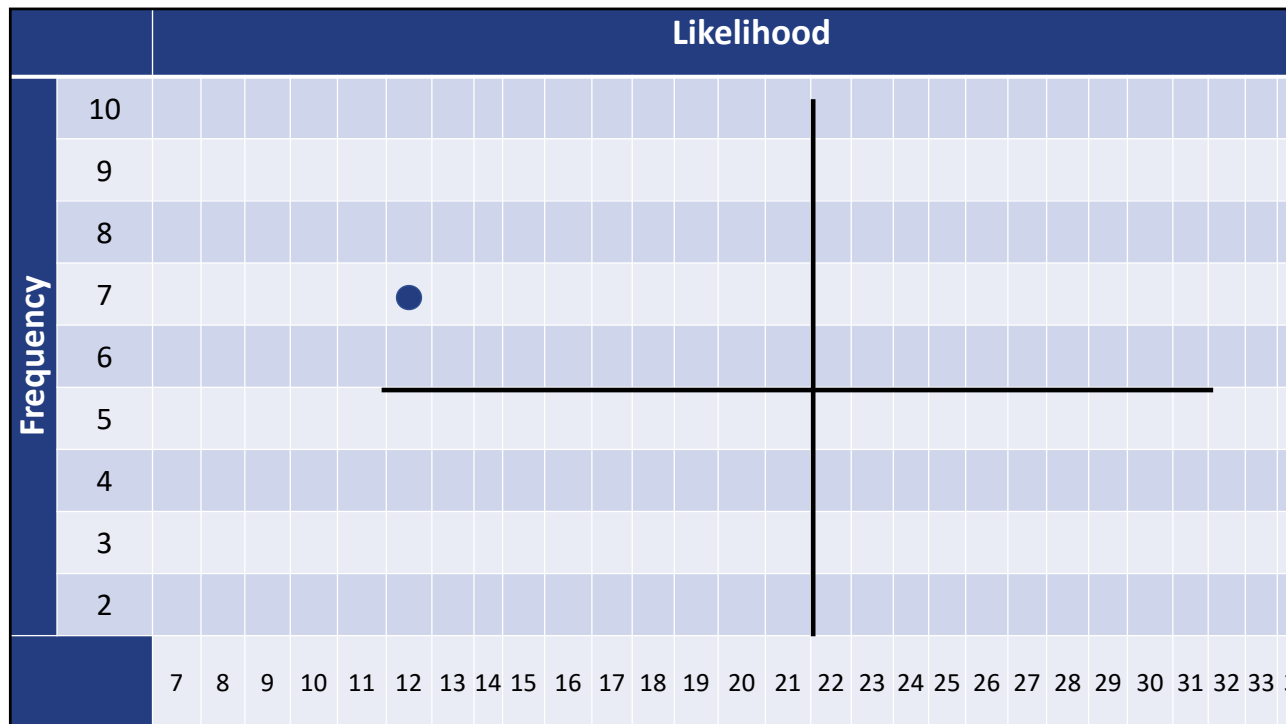
52

Likelihood of Occurrence Factors			
Rank/Scale		Measure of Likelihood	
		Existing Controls	Frequency of Noncompliance
1	Rare	<ul style="list-style-type: none"> • Policies mandated and updated regularly. • Regular mandatory training is provided to the identified responsible person(s) and is documented. • Regular management monitoring reviews are performed and documented. 	May only occur in exceptional circumstances Less than once in 10 years
2	Unlikely	<ul style="list-style-type: none"> • Policies mandated and updated regularly. • Regular training is provided to the identified responsible person(s), but not documented. • Regular management monitoring reviews are performed, but not documented. 	Could occur at some time At least once in 10 years
3	Possible	<ul style="list-style-type: none"> • Policies mandated, but not updated regularly. • Responsible person(s) identified. • Training is provided when needed. • Some management monitoring reviews are performed, but not documented. 	Might occur at some time At least once in 5 years
4	Likely	<ul style="list-style-type: none"> • Policies and procedures in place but neither mandated nor updated regularly. • Responsible person(s) identified. • Some formal and informal (on the job) training. • No management monitoring reviews. 	Will probably occur At least once per year
5	Almost Certain	<ul style="list-style-type: none"> • No controls in place. • No policies or procedures, no responsible person(s) identified, no training, and no management monitoring reviews. 	Expected to occur in most circumstances More than once per year

53

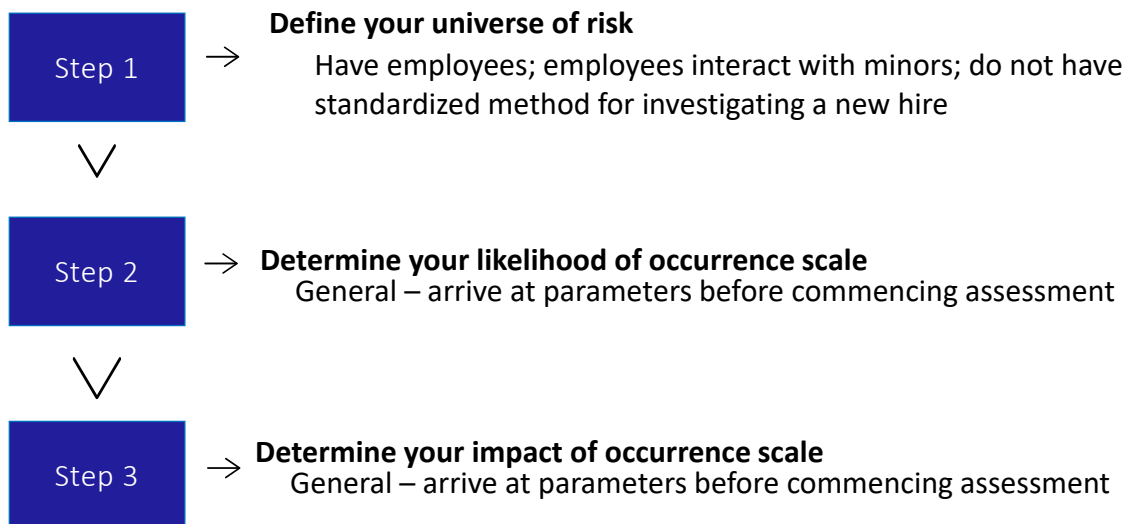
Impact of Occurrence Factors								
Rank/Scale		Measure of Impact						
		Legal/ Compliance	Health and Safety	Financial Monetary	Assets	Strategic	Potential Disruption of Business Operations	Reputation and Image
1	Insignificant	In compliance	No injuries	TBD dollar amount or percentage of budget	Little or no impact	Little or no impact	< ½ day	Unsubstantiated, low impact, low profile or no news items
2	Minor	Civil violation with little/no fines	First aid treatment	TBD dollar amount or percentage of budget	Minor loss or damage	Minor impact	< 1 day	Substantiated, low impact, low news profile
3	Serious	Significant civil fines/penalties	Medical treatment	TBD dollar amount or percentage of budget	Major damage	Major impact	1 day-1 week	Substantiated, public embarrassment, moderate impact, moderate news profile
4	Disastrous	Serious violation, criminal prosecution probable	Death or extensive injuries	TBD dollar amount or percentage of budget	Significant loss	Significant impact	1 week-1 month	Substantiated, public embarrassment, high impact, high news profile, third party actions
5	Catastrophic	Significant violation, criminal conviction probable, loss of accreditation or	Multiple deaths or several permanent disabilities	TBD dollar amount or percentage of budget	Complete loss of assets	Loss of accreditation or license	> 1 month	Substantiated, public embarrassment, very high multiple impacts, high widespread news profile, third party

54



55

Youth Protection Programs – Negligent Hiring



56

Negligent Hiring – Assessment Process

Step 4



Conducting Compliance Risk Survey

- Part I – what does your organization have in place – policy, procedure, training, etc.?
- Part II – what should your organization have in place?
- Part III – what risks have not been identified that are unique to your organization?



Step 5



Develop Compliance Universe Matrix (Heat Map)

- What is likelihood of occurrence?
 - Specific –
 - Do employees interact with minors?
 - Arrive at a numerical score
- What is impact of occurrence?
 - Specific
 - Type of business
 - Are there industry standards?
 - Does new hire have physical interaction with minors ?
 - Physical harm
 - Arrive at a numerical score

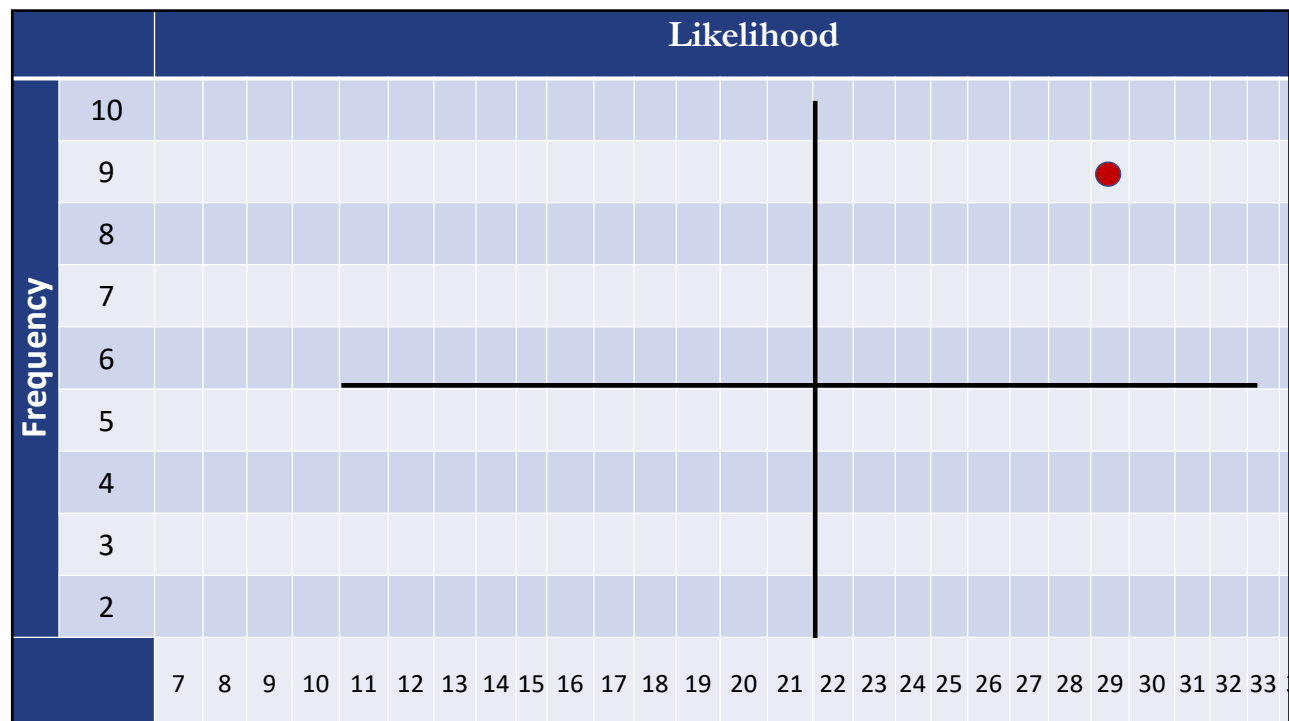
57

Likelihood of Occurrence Factors			
Rank/Scale		Measure of Likelihood	
		Existing Controls	Frequency of Noncompliance
1	Rare	<ul style="list-style-type: none"> Policies mandated and updated regularly. Regular mandatory training is provided to the identified responsible person(s) and is documented. Regular management monitoring reviews are performed and documented. 	May only occur in exceptional circumstances Less than once in 10 years
2	Unlikely	<ul style="list-style-type: none"> Policies mandated and updated regularly. Regular training is provided to the identified responsible person(s), but not documented. Regular management monitoring reviews are performed, but not documented. 	Could occur at some time At least once in 10 years
3	Possible	<ul style="list-style-type: none"> Policies mandated, but not updated regularly. Responsible person(s) identified. Training is provided when needed. Some management monitoring reviews are performed, but not documented. 	Might occur at some time At least once in 5 years
4	Likely	<ul style="list-style-type: none"> Policies and procedures in place but neither mandated nor updated regularly. Responsible person(s) identified. Some formal and informal (on the job) training. No management monitoring reviews. 	Will probably occur At least once per year
5	Almost Certain	<ul style="list-style-type: none"> No controls in place. No policies or procedures, no responsible person(s) identified, no training, and no management monitoring reviews. 	Expected to occur in most circumstances More than once per year

58

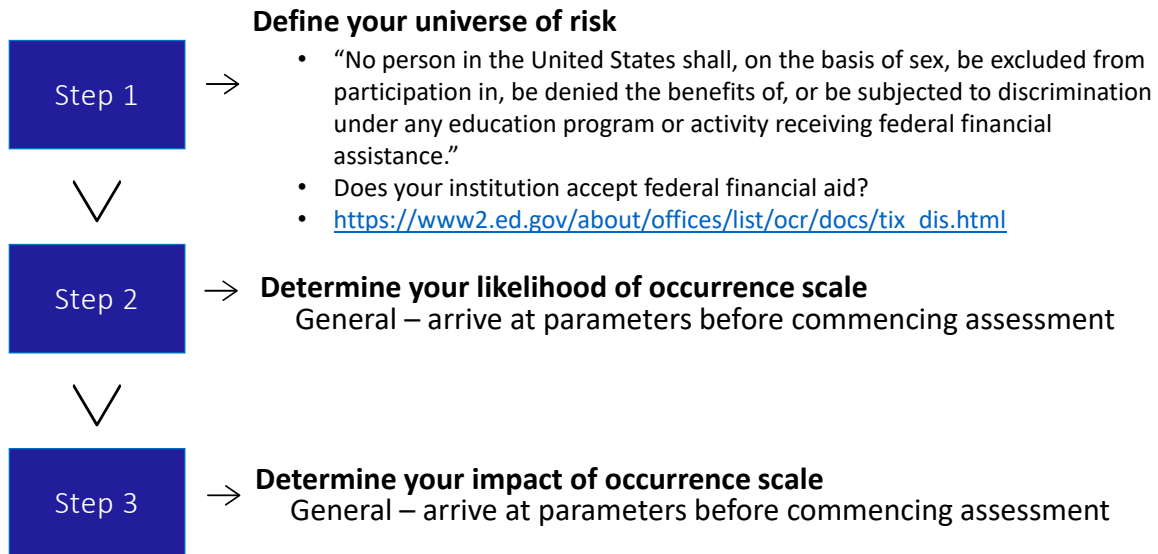
Impact of Occurrence Factors								
Rank/Scale		Measure of Impact						
		Legal/ Compliance	Health and Safety	Financial Monetary	Assets	Strategic	Potential Disruption of Business Operations	Reputation and Image
1	Insignificant	In compliance	No injuries	TBD dollar amount or percentage of budget	Little or no impact	Little or no impact	< ½ day	Unsubstantiated, low impact, low profile or no news items
2	Minor	Civil violation with little/no fines	First aid treatment	TBD dollar amount or percentage of budget	Minor loss or damage	Minor impact	< 1 day	Substantiated, low impact, low news profile
3	Serious	Significant civil fines/penalties	Medical treatment	TBD dollar amount or percentage of budget	Major damage	Major impact	1 day-1 week	Substantiated, public embarrassment, moderate impact, moderate news profile
4	Disastrous	Serious violation, criminal prosecution probable	Death or extensive injuries	TBD dollar amount or percentage of budget	Significant loss	Significant impact	1 week-1 month	Substantiated, public embarrassment, high impact, high news profile, third party actions
5	Catastrophic	Significant violation, criminal conviction probable, loss of accreditation or	Multiple deaths or several permanent disabilities	TBD dollar amount or percentage of budget	Complete loss of assets	Loss of accreditation or license	> 1 month	Substantiated, public embarrassment, very high multiple impacts, high widespread news profile, third party

59



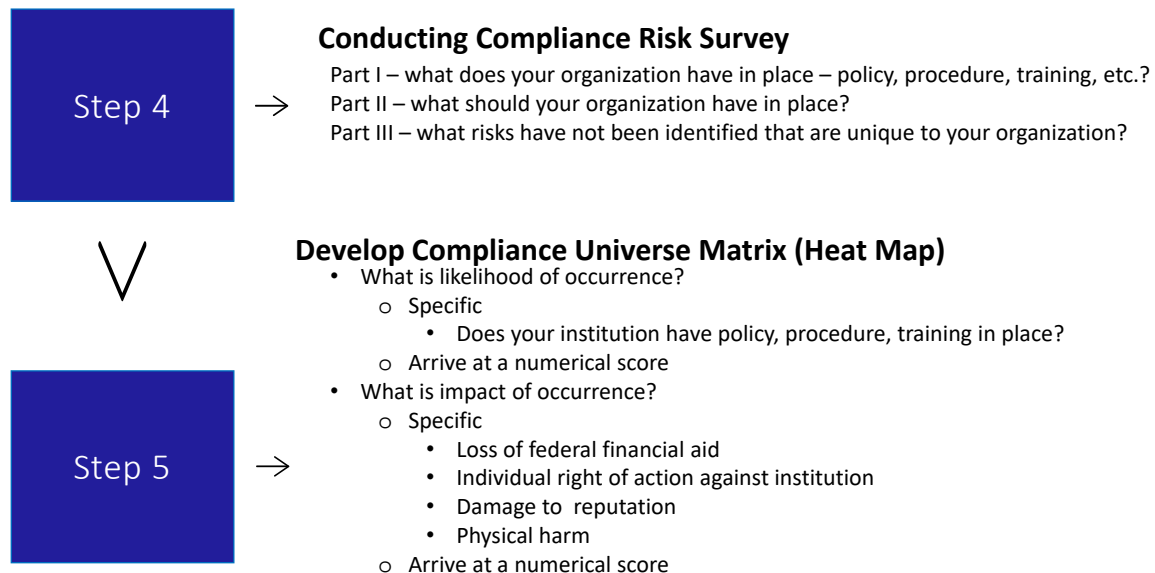
60

Title IX



61

Title IX – Assessment Process



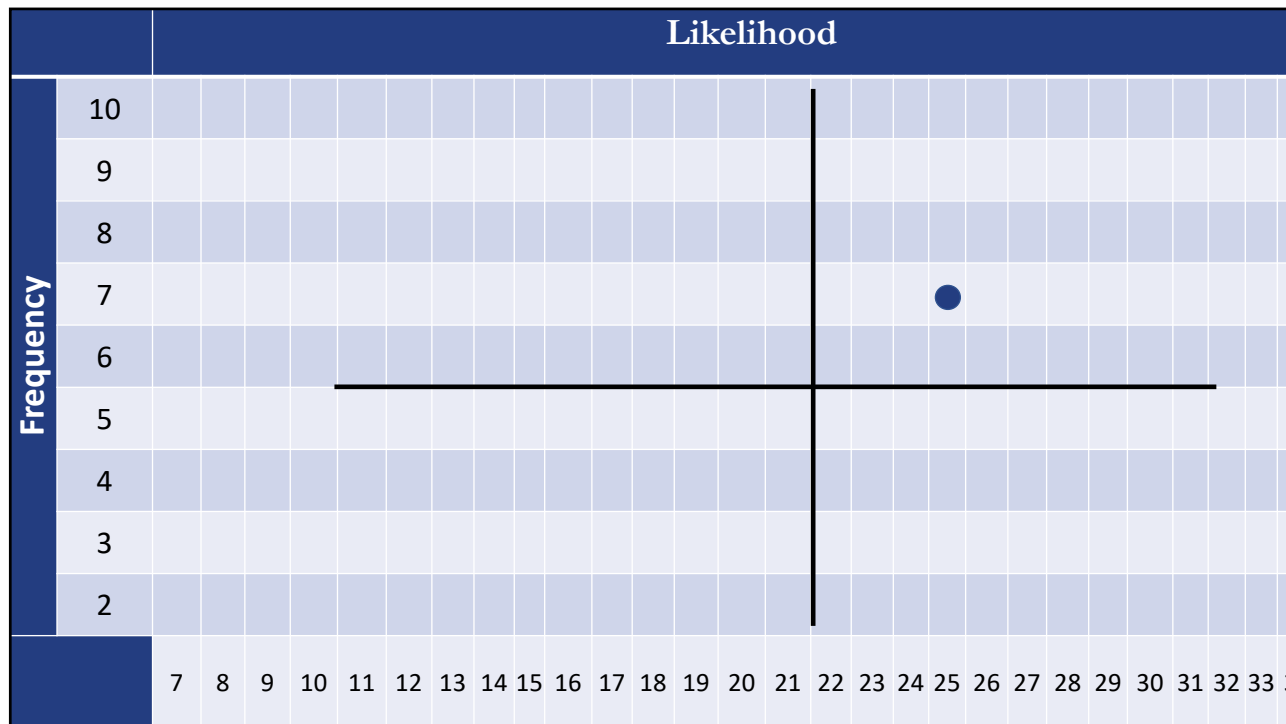
62

Likelihood of Occurrence Factors			
Rank/Scale		Measure of Likelihood	
		Existing Controls	Frequency of Noncompliance
1	Rare	<ul style="list-style-type: none"> • Policies mandated and updated regularly. • Regular mandatory training is provided to the identified responsible person(s) and is documented. • Regular management monitoring reviews are performed and documented. 	May only occur in exceptional circumstances Less than once in 10 years
2	Unlikely	<ul style="list-style-type: none"> • Policies mandated and updated regularly. • Regular training is provided to the identified responsible person(s), but not documented. • Regular management monitoring reviews are performed, but not documented. 	Could occur at some time At least once in 10 years
3	Possible	<ul style="list-style-type: none"> • Policies mandated, but not updated regularly. • Responsible person(s) identified. • Training is provided when needed. • Some management monitoring reviews are performed, but not documented. 	Might occur at some time At least once in 5 years
4	Likely	<ul style="list-style-type: none"> • Policies and procedures in place but neither mandated nor updated regularly. • Responsible person(s) identified. • Some formal and informal (on the job) training. • No management monitoring reviews. 	Will probably occur At least once per year
5	Almost Certain	<ul style="list-style-type: none"> • No controls in place. • No policies or procedures, no responsible person(s) identified, no training, and no management monitoring reviews. 	Expected to occur in most circumstances More than once per year

63

Impact of Occurrence Factors								
Rank/Scale		Measure of Impact						
		Legal/ Compliance	Health and Safety	Financial Monetary	Assets	Strategic	Potential Disruption of Business Operations	Reputation and Image
1	Insignificant	In compliance	No injuries	TBD dollar amount or percentage of budget	Little or no impact	Little or no impact	< ½ day	Unsubstantiated, low impact, low profile or no news items
2	Minor	Civil violation with little/no fines	First aid treatment	TBD dollar amount or percentage of budget	Minor loss or damage	Minor impact	< 1 day	Substantiated, low impact, low news profile
3	Serious	Significant civil fines/penalties	Medical treatment	TBD dollar amount or percentage of budget	Major damage	Major impact	1 day-1 week	Substantiated, public embarrassment, moderate impact, moderate news profile
4	Disastrous	Serious violation, criminal prosecution probable	Death or extensive injuries	TBD dollar amount or percentage of budget	Significant loss	Significant impact	1 week-1 month	Substantiated, public embarrassment, high impact, high news profile, third party actions
5	Catastrophic	Significant violation, criminal conviction probable, loss of accreditation or	Multiple deaths or several permanent disabilities	TBD dollar amount or percentage of budget	Complete loss of assets	Loss of accreditation or license	> 1 month	Substantiated, public embarrassment, very high multiple impacts, high widespread news profile, third party

64








65



66

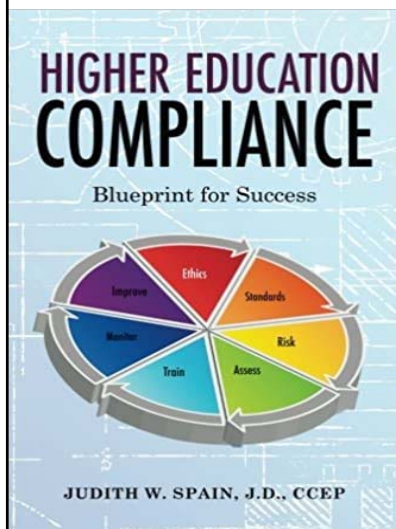
Action Items

-  Determine level of top support for risk assessment initiative;
-  Identify structure of risk assessment initiative;
-  Develop universe of risk;
-  Use standardized assessment tools to develop heat map;
-  Complete assessment process.



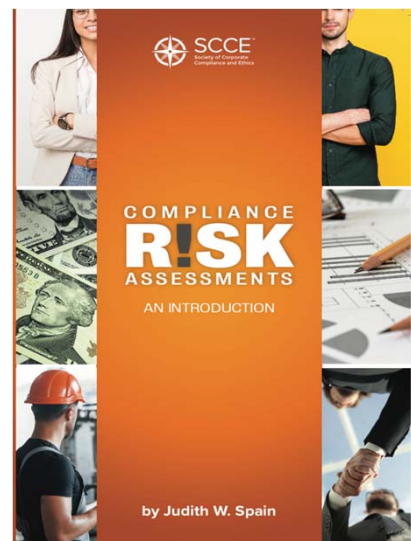
67

Judith W. Spain J.D., CCEP



HECC

Higher
Education
Compliance
Consulting



jspain@higheredcomplianceconsulting.com

<https://www.higheredcomplianceconsulting.com>

(859)582-9451

68