FirstKey HOMES™

Mapping Ethical Risk

Joint IIA / GACFE Meeting
August 12, 2022

Elizabeth Simon, CPA, CFE, LPEC, CCEP, CIPP-US, SHRM-CP
VP, Compliance

FirstKey HOMES™

Elizabeth Simon

Vice President, Compliance

My responsibilities:

- Regulatory Compliance
- Business Licensing
- Enterprise Risk Management
- Environmental, Social, Governance Program
- Privacy Program

Agenda

1 Back to the Basics

- Inherent vs Residual Risk
- Enterprise Risk Assessments

2 Why is this Important?

- DOJ Guidance for Compliance Programs

3 Compliance in ERAs

- Compliance Risk Assessments

4 How to Incorporate Ethics

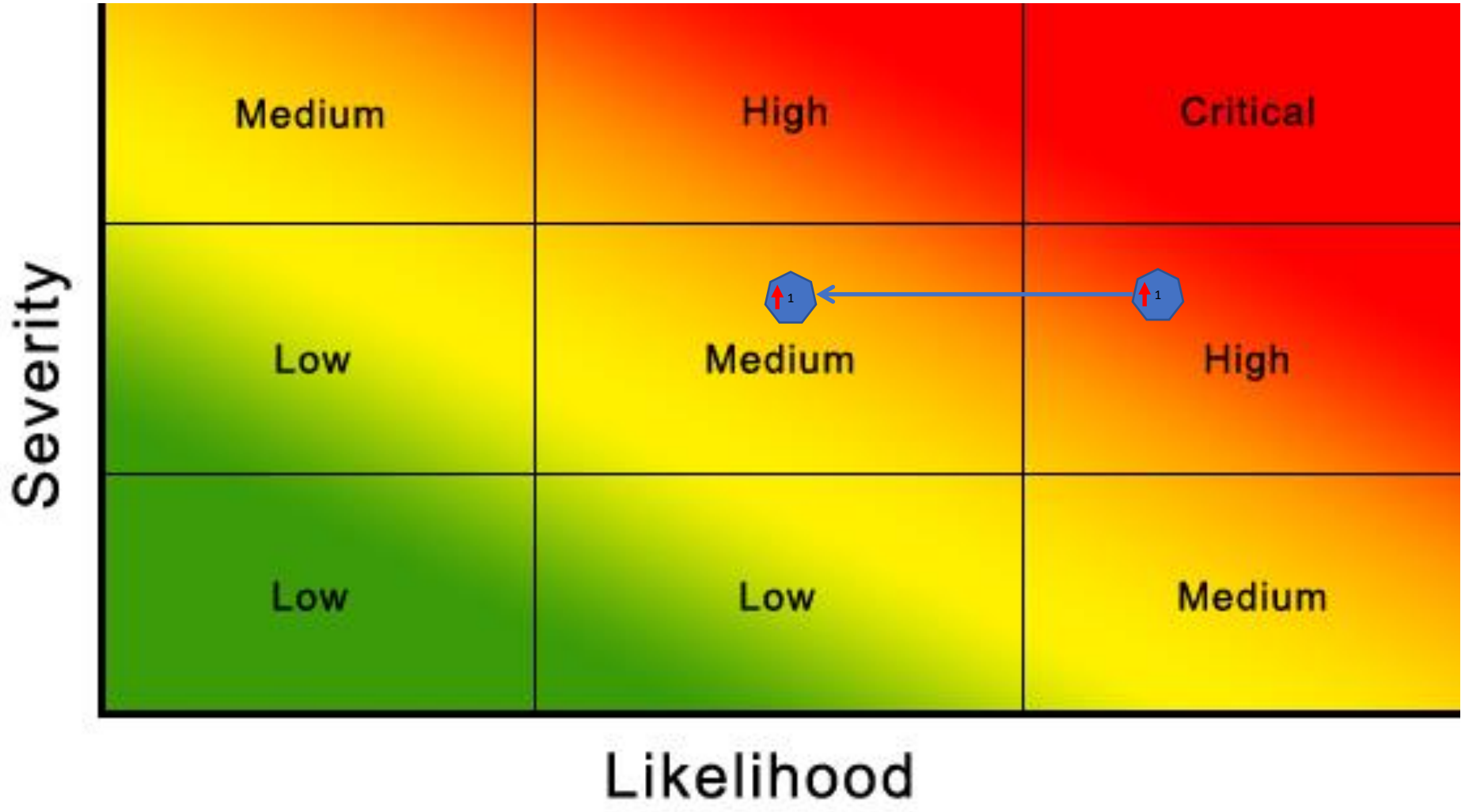
- Example assessments

5 What Now?

- How to take this back and apply it

Back to the Basics

Inherent Risk vs. Residual Risk



Four Areas of Enterprise Risk

Examples:
- Organizational Structure
- Competitive Risk
- Culture/Ethics
- Reputational Risk
- Customer Priority Shifts
- Succession Planning
- Risk Response Perception
- Geopolitical Risk
- Economic Risk
- Values Misalignment
- Demographic Changes

Examples:
- Spread of Infectious Diseases
- Second Wave of COVID-19
- Customer bankruptcy
- Quality Risk
- Incentives Risk
- Diversity
- Information Technology
- Cybersecurity
- Business Continuity
- Disaster Recovery
- Supply Chain Risk
- Research and Development Risk

Examples:
- Generally Accepted Accounting Principles Compliance
- Fraud
- Capital/Liquidity Risk
- Credit Risk
- Unmanageable Inflation
- Financial Reporting Structure
- Financial Systems
- Transaction Complexity
- Taxation Risk
- Interest Rate Risk
- Restatement Risk

Examples:
- Bribery/corruption
- Third Party Compliance Risk
- Records Management Regulations
- General Regulatory Compliance Risks
- Health and Safety Regulations
- Product Regulations
- Environmental Regulations
- Social Compliance Regulations
- Employment Laws
- Whistleblower Protections
- Intellectual Property
- Legal Liability

When looking at Enterprise Risk, you must look at all risks across the four main categories, and identify where Compliance owns some or all of the risk for the company.

Why is this Important?

“Risk Assessment” in the 2020 DOJ Guidance

- The word “risk” is mentioned 53 times in the 2020 DOJ guidance.
- “Risk assessment” has its own dedicated section.

“The starting point for a prosecutor’s evaluation of whether a company has a well-designed compliance program is to understand the company’s business from a commercial perspective, how the company has identified, assessed, and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks.”

“Risk Assessment” in the 2020 DOJ Guidance

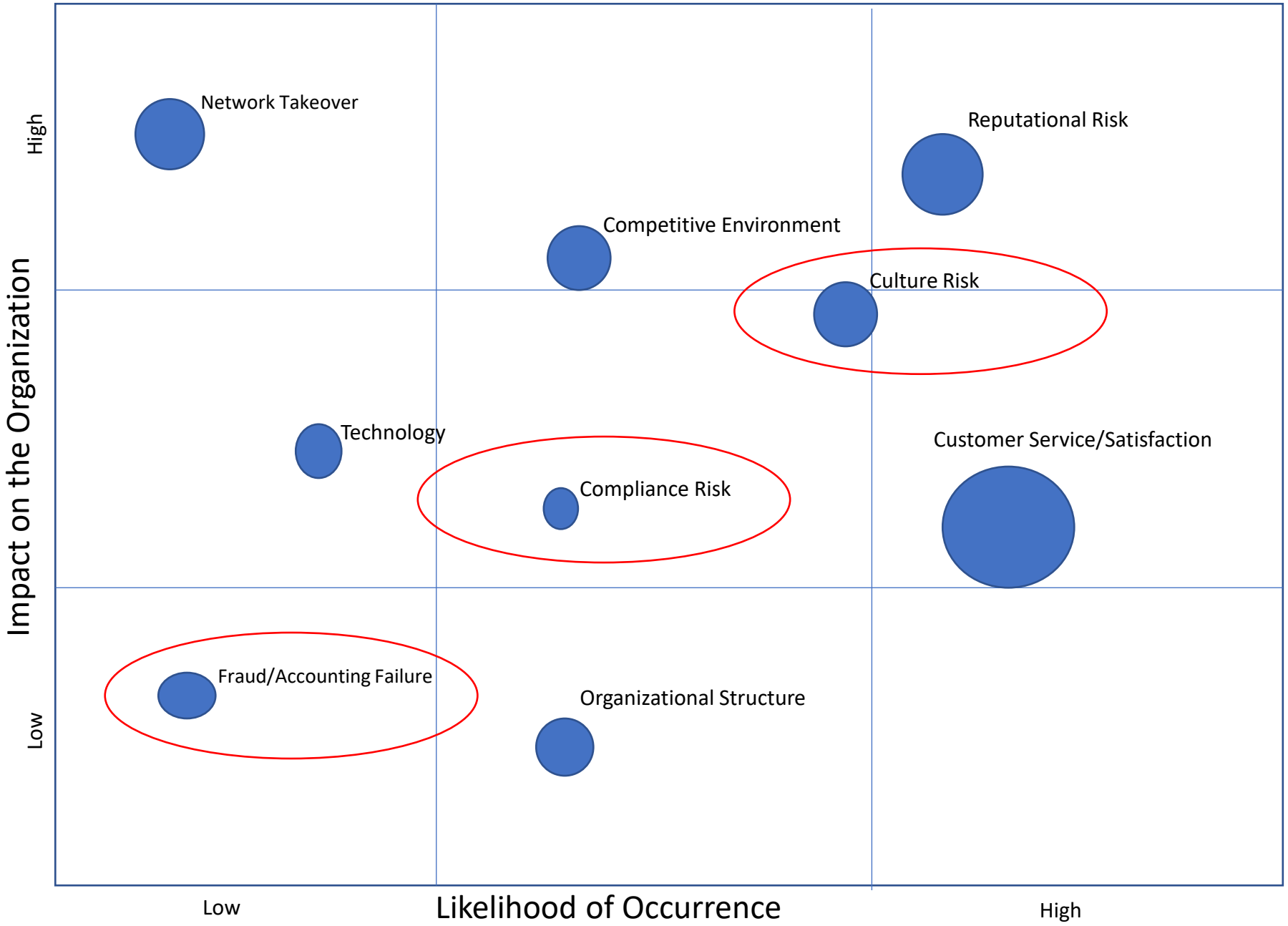
DOJ Guidance

- Justice Manual, “Principles of Federal Prosecution of Business Organizations” (the “Filip Factors”)
  - 8 Factors, including **Risk Assessment**, **Incentives**, and **Training & Communications**
  - Applies specifically to Criminal Anti-Trust, but top officials have indicated they will be considered for all other Criminal Division matters, as well as some or all Civil Division matters.

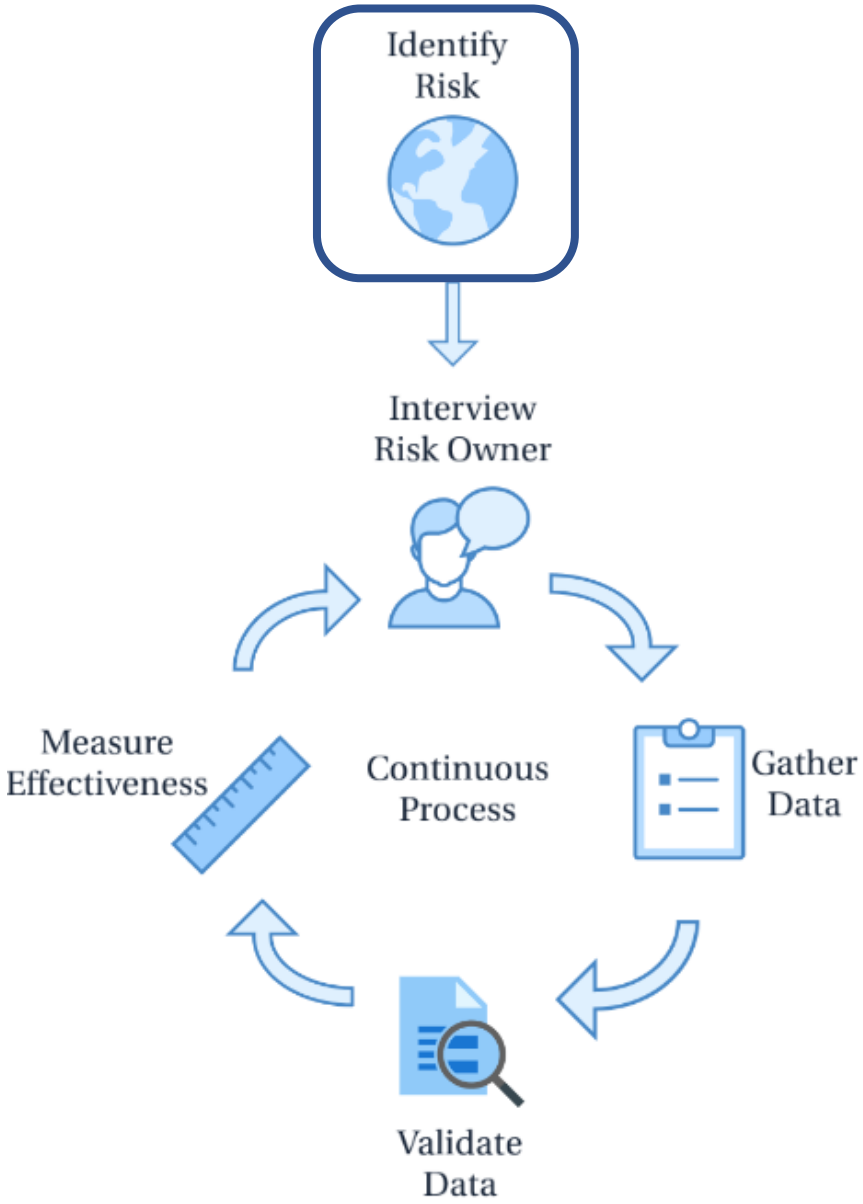
“If senior management does not actively support and cultivate a culture of compliance, a company will have a paper compliance program, not an effective one.”

Incorporating Compliance into ERM

Enterprise Risk Management Model



Identify the Risks in Your Risk Universe



Likelihood of a Violation

- Annual Frequency
- Probability of Occurrence
- Complexity
- Business Units Involved
- Hotline Cases
- Country Risk
- Department Risk

Impact of a Violation

- Financial Loss
- Fines/Penalties
- Reputational Impact
- Employee Morale

Velocity of Risk

- Level of federal enforcement
- Fines/penalties against competitors
- Significant legislation
- Media spotlight

Effectiveness of Controls

- Policies/Procedures
- Training
- Monitoring
- Internal Audit Results
- Management's Response

Sample Compliance Risk Universe

Labor Relations & Employment

Wage and Hour Laws
- Fair Labor Standards Act (FLSA)
- Family and Medical Leave Act (FMLA)
- Consumer Credit Protection Act (CPCA)
- Employee Polygraph Protection Act

Employee Benefit Security
- Employee Retirement Income Security Act (ERISA)
- Comprehensive Omnibus Budget Reconciliation Act of 1985 (COBRA)
- Health Insurance Portability and Accountability Act (HIPPA)

Unions
- National Labor Relations Act (NLRA)
- Labor-Management Reporting and Disclosure Act (MLRDA) / Landrum-Griffin Act

Government Contracts

- Contract Work Hours and Safety Standards Act
- Davis-Bacon and Related Acts
- Copeland Act
- False Claims Act
- FAR 52 Compliance
- E-Verify
- Most Favored Nations Clause

Antitrust Compliance

- Sherman Act
- Robinson-Patman Act
- Clayton Act
- Truth in Billing

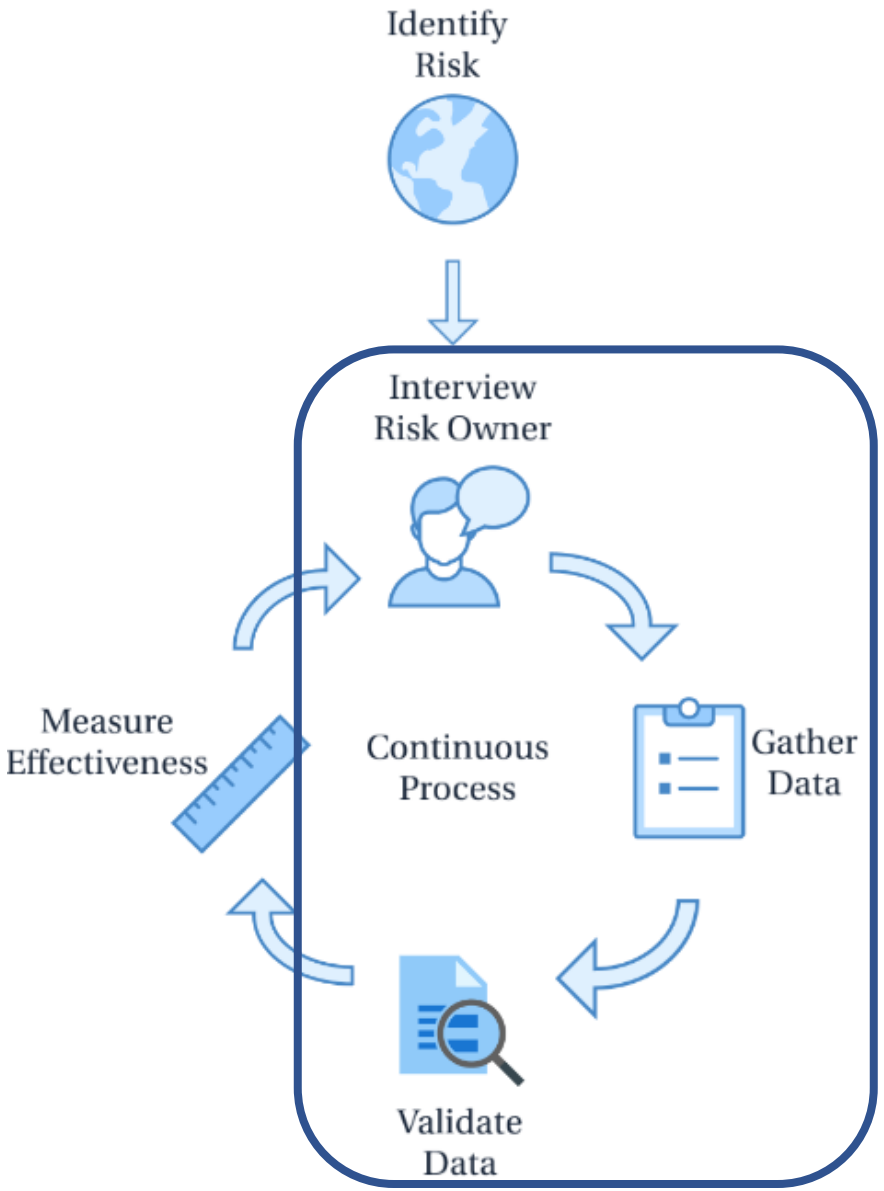
Data Protection & Privacy

- Gramm Leach Bliley Act
- Payment Card Industry compliance
- Children's Online Privacy Protection Rule (16 C.F.R. §312)
- Communication Assistance for Law Enforcement Act (CALEA – 18 USC §2510)
- Electronic Communications Privacy Act (18 USC §2701)

Sales/Marketing Compliance

- Consumer Leasing Act
- CAN-Spam Act
- Truth in Advertising

Gather and Validate Your Data



Likelihood of a Violation

- Annual Frequency
- Probability of Occurrence
- Complexity
- Business Units Involved
- Hotline Cases
- Country Risk
- Department Risk

Impact of a Violation

- Financial Loss
- Fines/Penalties
- Reputational Impact
- Employee Morale

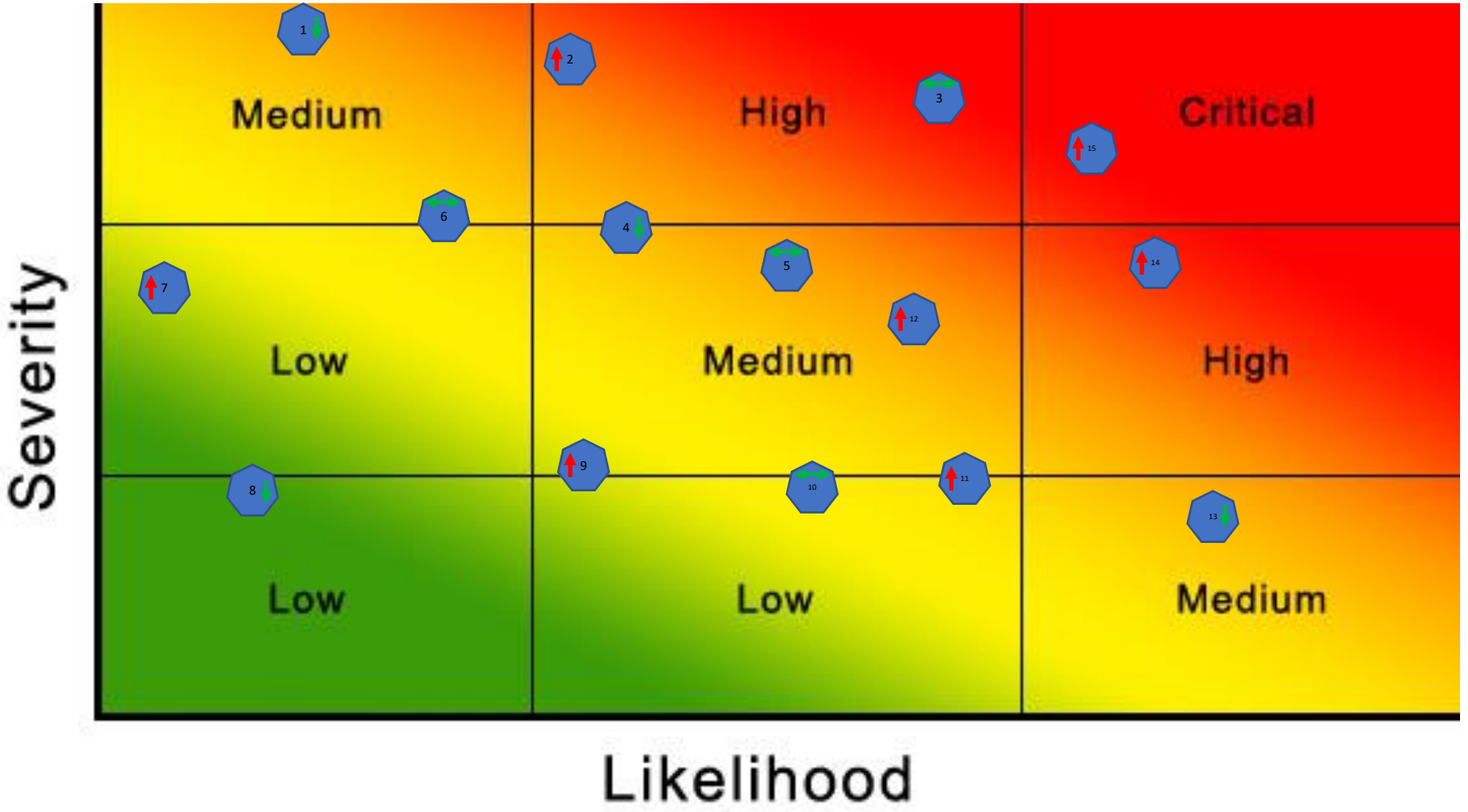
Velocity of Risk

- Level of federal enforcement
- Fines/penalties against competitors
- Significant legislation
- Media spotlight

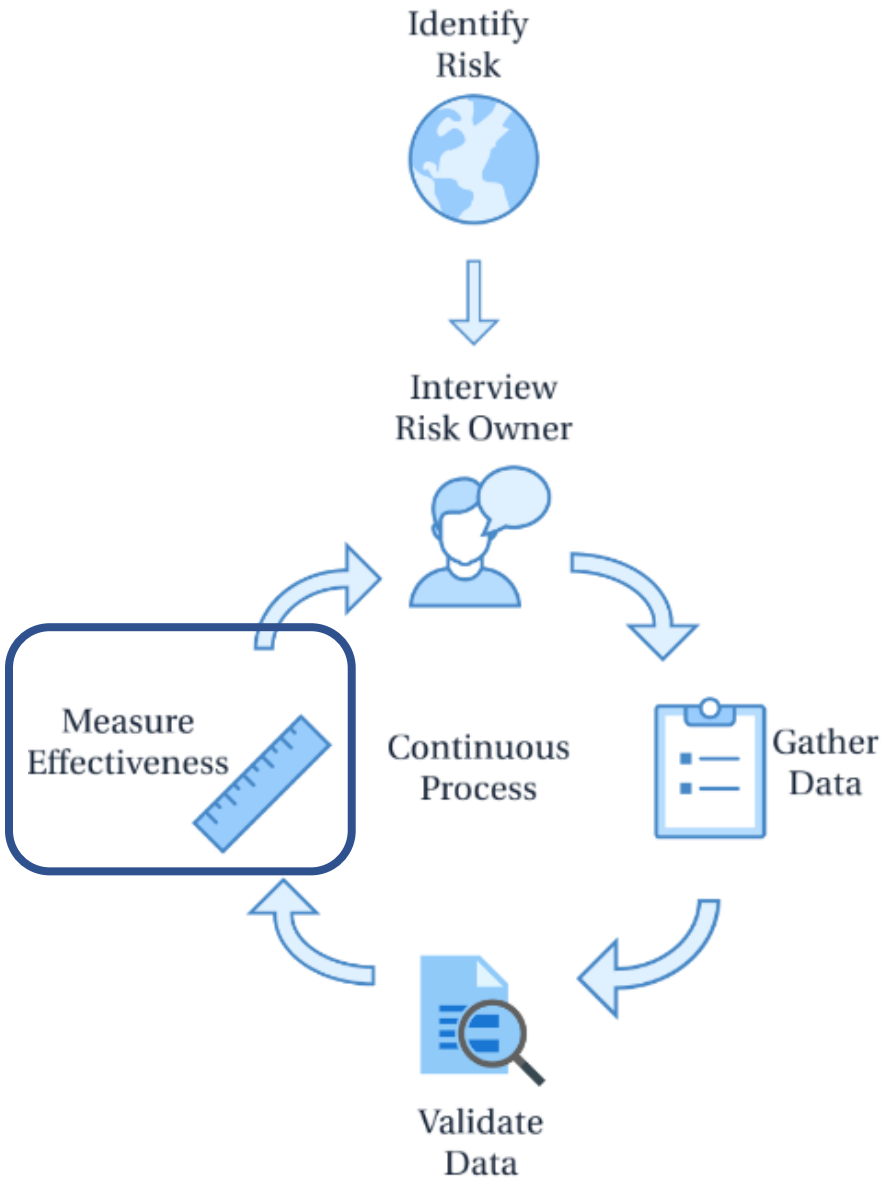
Effectiveness of Controls

- Policies/Procedures
- Training
- Monitoring
- Internal Audit Results
- Management's Response

Compliance Risk Heat Map – Inherent Risk



Measure Effectiveness of Your Controls



Likelihood of a Violation

- Annual Frequency
- Probability of Occurrence
- Complexity
- Business Units Involved
- Hotline Cases
- Country Risk
- Department Risk

Impact of a Violation

- Financial Loss
- Fines/Penalties
- Reputational Impact
- Employee Morale

Velocity of Risk

- Level of federal enforcement
- Fines/penalties against competitors
- Significant legislation
- Media spotlight

Effectiveness of Controls

- Policies/Procedures
- Training
- Monitoring
- Internal Audit Results
- Management's Response

Compliance Risk Assessment Scorecard

Program Element	Green	Yellow	Red
Oversight	The program has a clear owner that provides reports on a regular basis to the Office of the Chief Compliance Officer	The program has an owner, but does not provide reports to the Office of the Chief Compliance Officer	The program does not have a clear owner
Due Diligence / Communication	Background check is conducted on all employees' time of hire in accordance with company's employment requirements. Relevant employees receive additional screening at time of internal transfer or promotion to confirm background screen and review of existing personnel file and Ethics Line database; review does not indicate that individual hired/promoted has engaged in illegal conduct or other conduct that is inconsistent with an effective compliance program.	Background check is conducted at time of hire but not at time of internal transfer from a non-relevant role to a relevant role or at the time of promotion within relevant roles.	Background checks have not been conducted for all new hires, internal transfers, and promotions, are performed using inconsistent standards between hiring locations, or negative background results are ignored
Disciplinary Action	The policy clearly states that all employees found to be intentionally non-compliant are disciplined or separated, and all employees found to be unknowingly non-compliant are disciplined or retrained.	The policy is in place, but some employees found to be non-compliant have not been adequately disciplined.	There is no policy in place regarding enforcement and discipline due to non-compliance.
Risk Assessment	Yes. A risk assessment has been completed specifically around this topic area in the past 2 years	Yes. This topic area has been included in a general compliance risk assessment that has been completed in the past 2 years	No. A risk assessment has not been completed in over 2 years
Auditing	The compliance program has been audited by an independent audit function, such as Internal Audit within the last year	The compliance program has been audited by an independent audit function, such as Internal Audit within the past two years	The compliance program has not been audited by an independent audit function in over two years.
	No non-conformances/issues were detected through audits	Less than 5 minor non-conformances to legal requirements	One or more major non-conformances to legal requirements
Enforcement Actions	0 investigations/charges per year	1 investigation/charge per year	More than 1 investigation/charge per year
	There are no damages, settlements, or fines from litigation due to compliance failures	Total damages, settlements, and fines from litigation due to compliance failures is within 5% (+ or -) of target	Total damages, settlements, and fines from litigation due to compliance failures is greater than 5% (+ or -) of target
	There are no new lawsuits filed against the company/open litigation matters	Number of new lawsuits filed against the company/open litigation matters is within 5% (+ or -) of target	Number of new lawsuits filed against the company/open litigation matters is greater than 5% (+ or -) of target

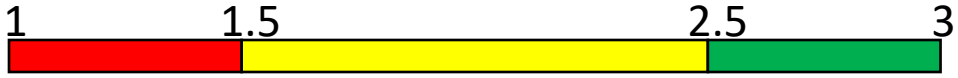
Compliance Risk Assessment Scorecard

Program Element	Green	Yellow	Red
Standards & Procedures	The policy/M&Ps are in place and have been reviewed in the past year	The policy/M&Ps are in place, but have not been reviewed in over a year	No corporate policy/M&Ps exists
	The policy/M&Ps are available to 100% of relevant employees	Greater than 90% of relevant employees have read and understand the policy/M&Ps	The M&Ps are not available to all relevant employees or less than 90% of employees have read and understand the policy
Training & Education	Trainings are mandatory and available to all relevant employees for understanding all relevant compliance laws	Yes, trainings are available, but are not mandatory and/or are not in a format that will reach all relevant employees	No, trainings are not available
	100% of relevant employees complete the available training courses	Greater than 90% of relevant employees complete the available training courses	Less than 90% of relevant employees complete the available training courses
Monitoring	There is a process in place to regularly (more than once a year) internally monitor compliance with applicable laws	The compliance program has been internally monitored within the last year	There is no current monitoring being conducted
	No non-conformances/issues were detected through audits	Less than 5 minor non-conformances to legal requirements	One or more major non-conformances to legal requirements
Corrective Action	The spending level on compliance activities is within budget	The spending level on compliance activities is within 5% (+ or -) of budget	The spending level on compliance activities is greater than 5% (+ or -) of budget
	Less than 90 days	Between 90 and 120 days	Greater than 120 days

Compliance Summary Scorecard

	Program Element								
Compliance Area	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Area Total**
Labor Relations and Employment									
Government Contracts									
Antitrust Compliance									
Data Protection and Privacy									
Sales/Marketing Compliance									

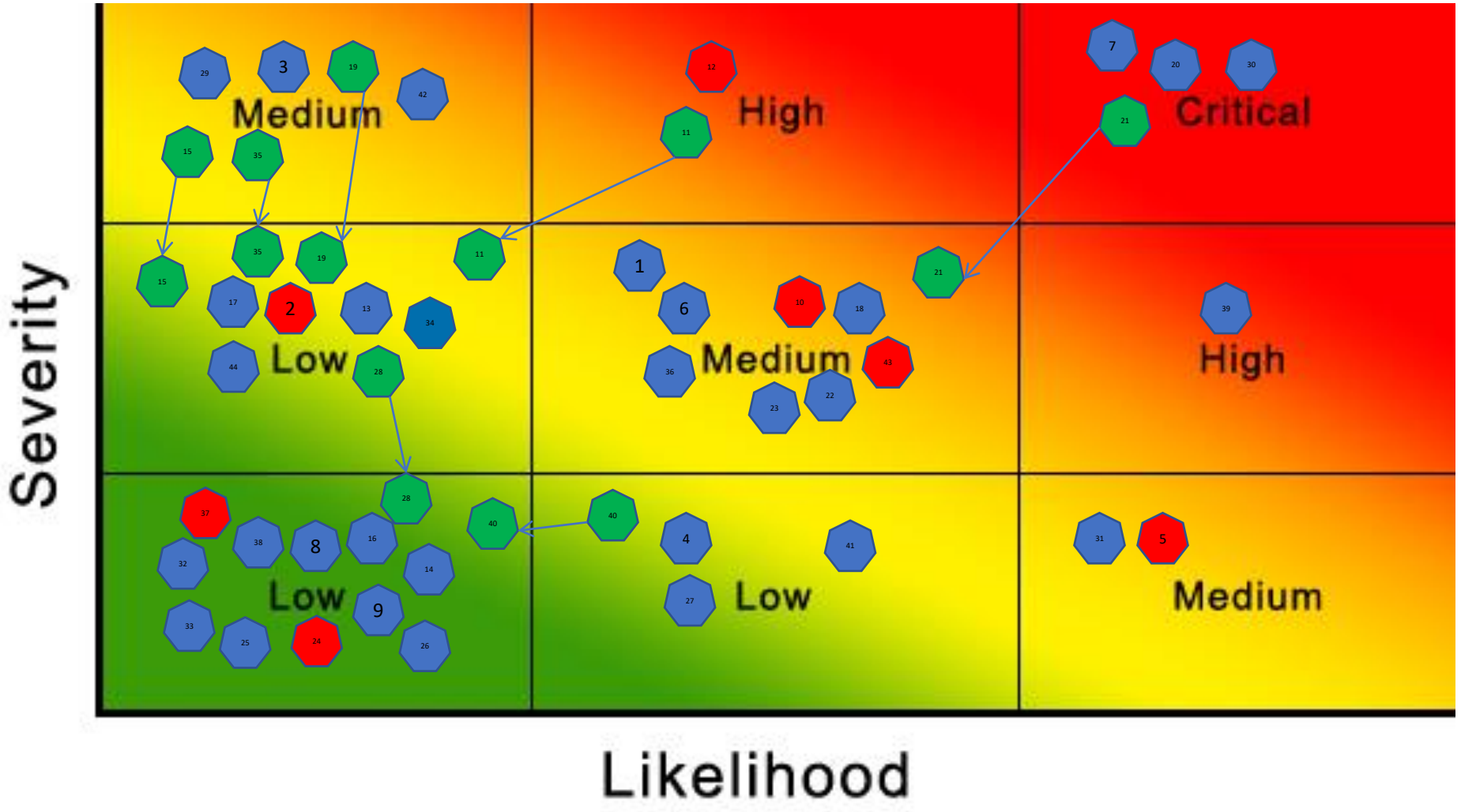
Rating Scale:



1 - Standards and Procedures
2 - Oversight - Compliance Officer or Compliance Committee
3 - Due Diligence/Open Lines of Communication
4 - Training and Education

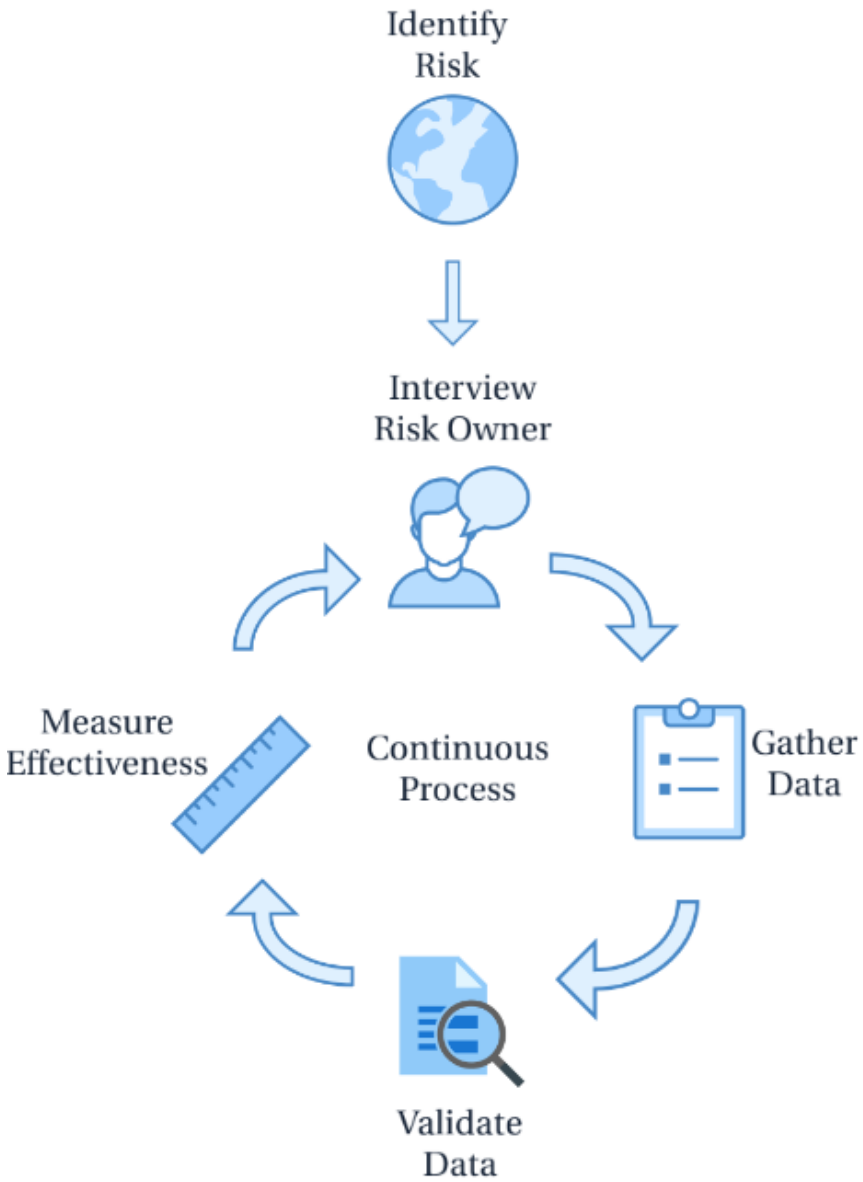
5 - Auditing and Monitoring
6 - Enforcement and Disciplinary
7 - Corrective Action Procedures (Response and Prevention)
8 – Risk Assessment

Compliance Risk Heat Map – Residual Risk



Incorporating Ethics into ERM

Analyze the Scope of the Risk



Likelihood of a Violation

- Annual Frequency
- Probability of Occurrence
- Complexity
- Business Units Involved
- Hotline Cases
- Country Risk
- Department Risk

Impact of a Violation

- Financial Loss
- Fines/Penalties
- Reputational Impact
- Employee Morale

Velocity of Risk

- Level of federal enforcement
- Fines/penalties against competitors
- Significant legislation
- Media spotlight

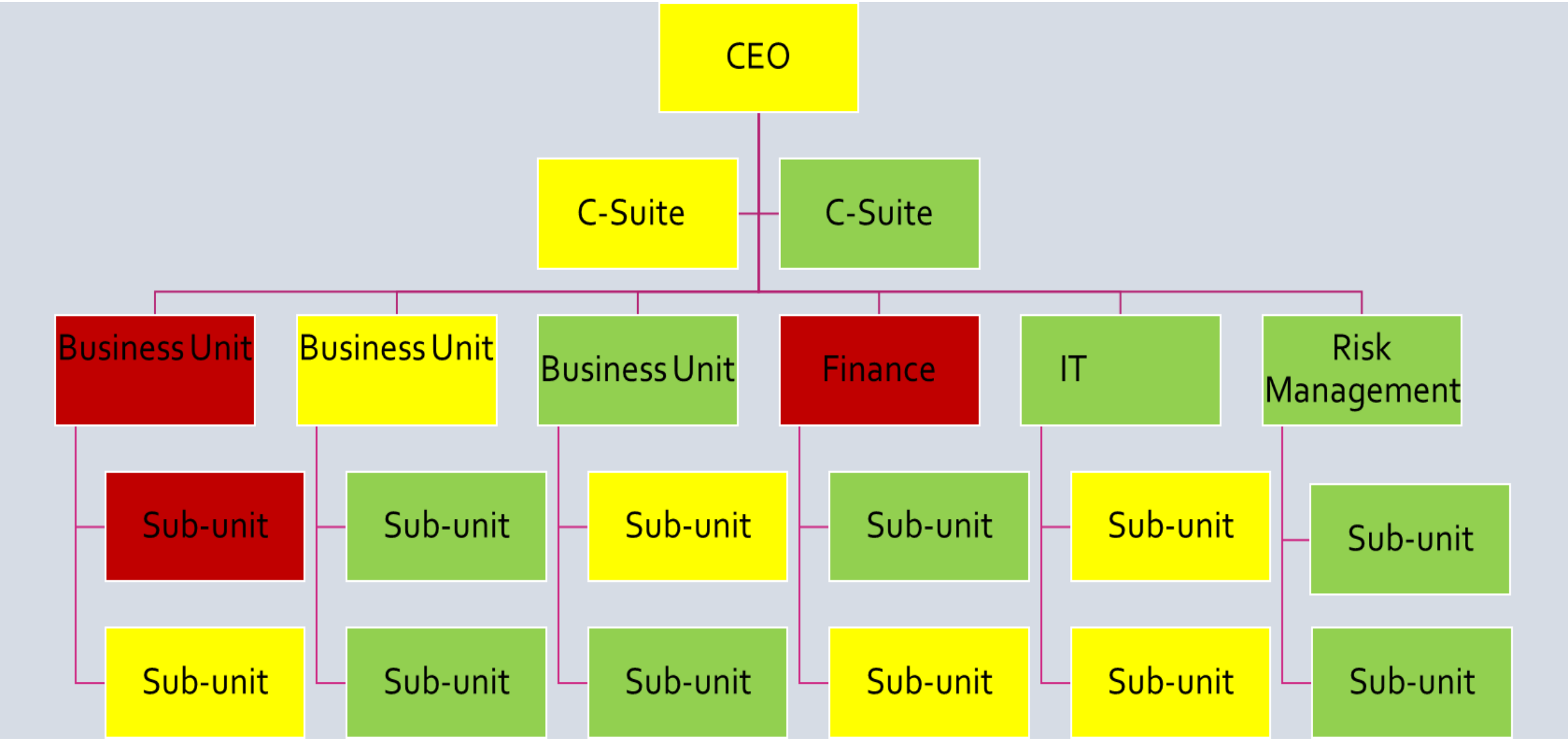
Effectiveness of Controls

- Policies/Procedures
- Training
- Monitoring
- Internal Audit Results
- Management's Response

Ethical Considerations

- Number of alerts generated for policy violations (Travel & Expense; Employee Fraud; Harassment/Discrimination; Bribery, Corruption & Insider Trading; Customer and Vendor Complaints; etc.)
- Number of Hotline complaints
- Training statistics (promptness in taking mandatory training, question-level analysis of success rates, level of participation in non-mandatory training)
- Assess across units (what culture problems do you have and where do you have them)
  - Certain business functions and job categories present a higher level of risk in terms of ethical behavior – Sales; Vendor Management; Trading; etc.
- Focus on level of seniority – Are they leading by example?

Department Risk

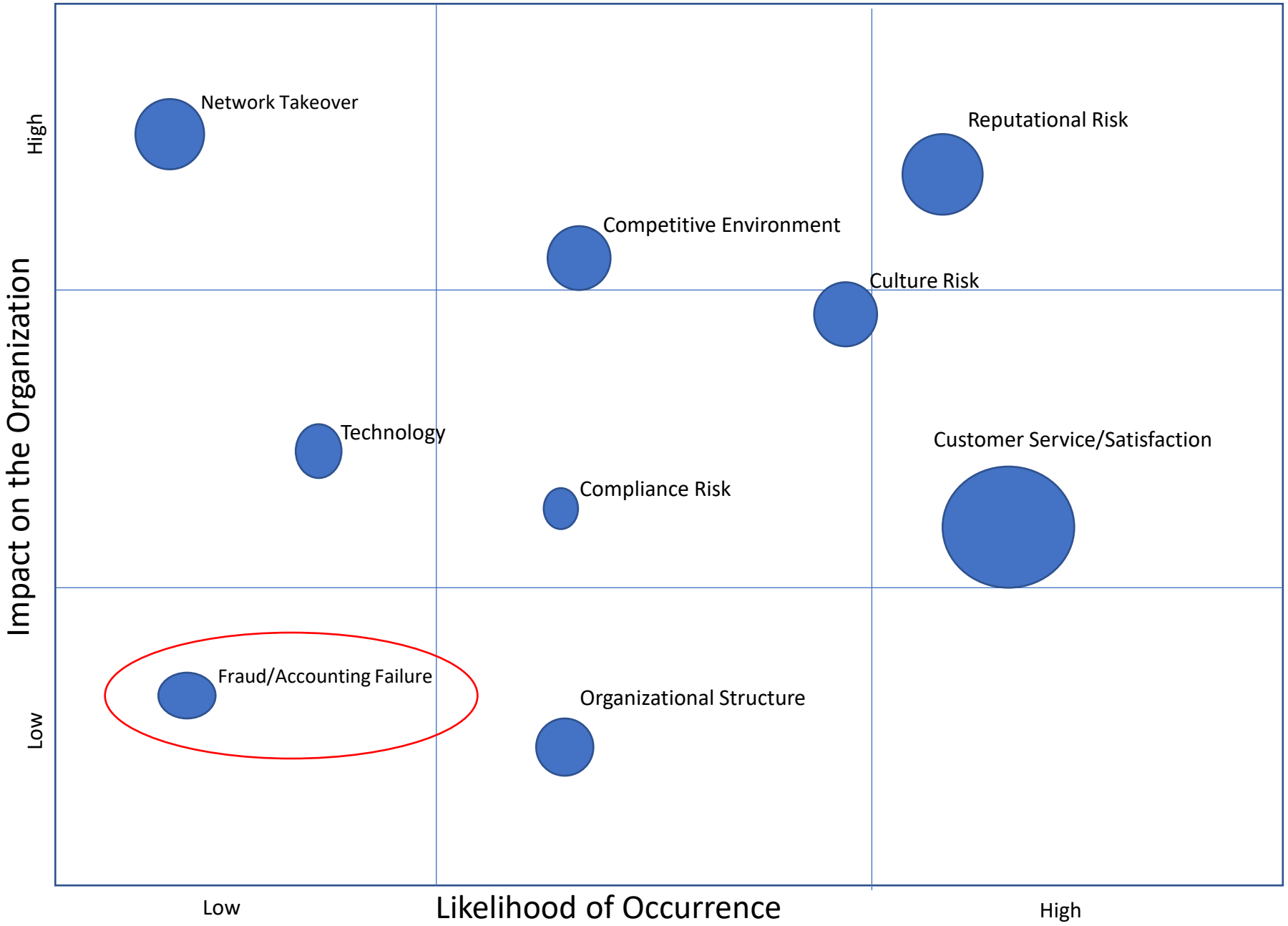


Ethical Considerations

- Remote from Manager
- Manage Has Large Span of Control
- Top Performer
- Marginal Performer
- Third Party Selection / Assessment
- Vendor / Counterparty / Due Diligence
- Regulated Activity
- Overseas Market
- High Risk Market
- Signing Authority and Level
- Market Share
- Objectivity required
- Deals with Politically Exposed Persons (PEPs)

Putting it all Together

Enterprise Risk Management Model

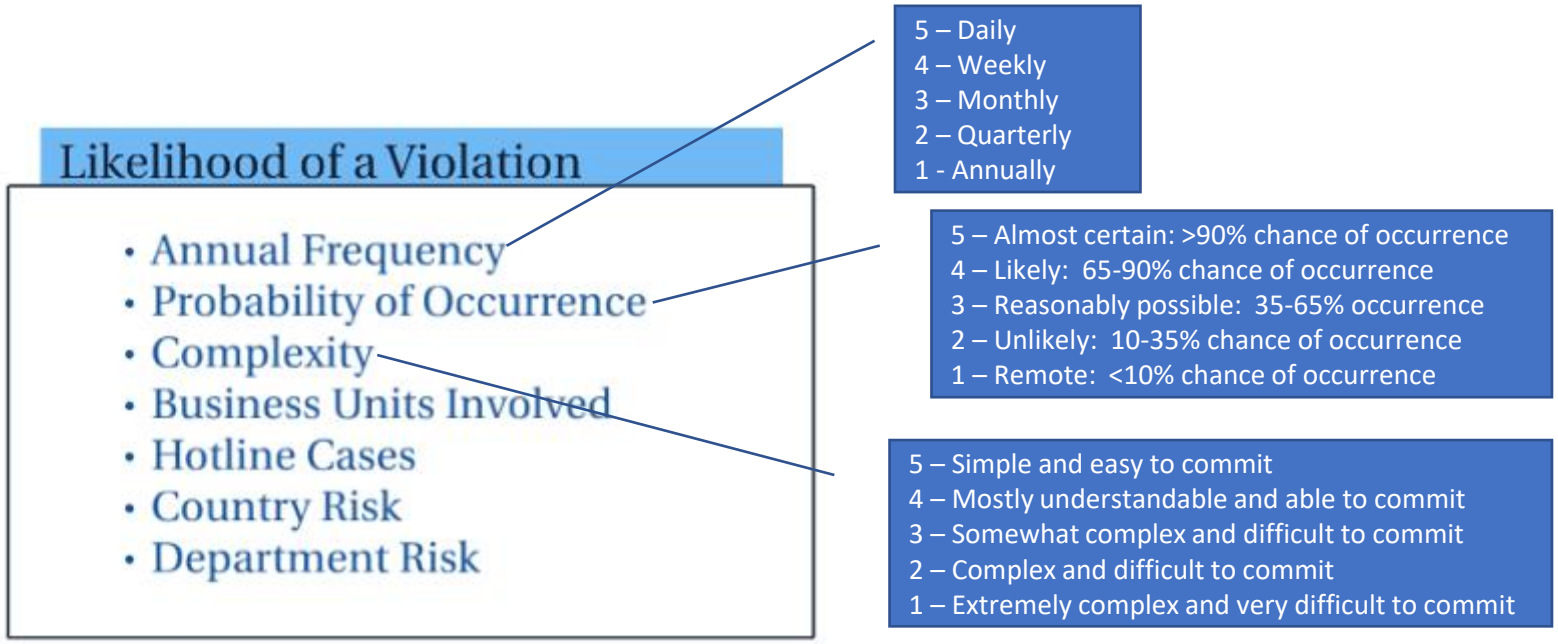


Example Fraud Risks

Fraud Risk Level 1	Fraud Risk Level 2	Risk Description
Cash	Larceny	The risk that an individual in the company steals cash from register
Fraudulent Disbursements	Billing Scheme	The risk that vendors could be added to the vendor master or modified within the vendor master without a valid reason or approval, causing an increased risk of fraud.
Billing Scheme	Personal Purchases	Personal purchases with company funds through the A/P system

Assess the Likelihood

Risk Description: The risk that an individual in the company steals cash from register.

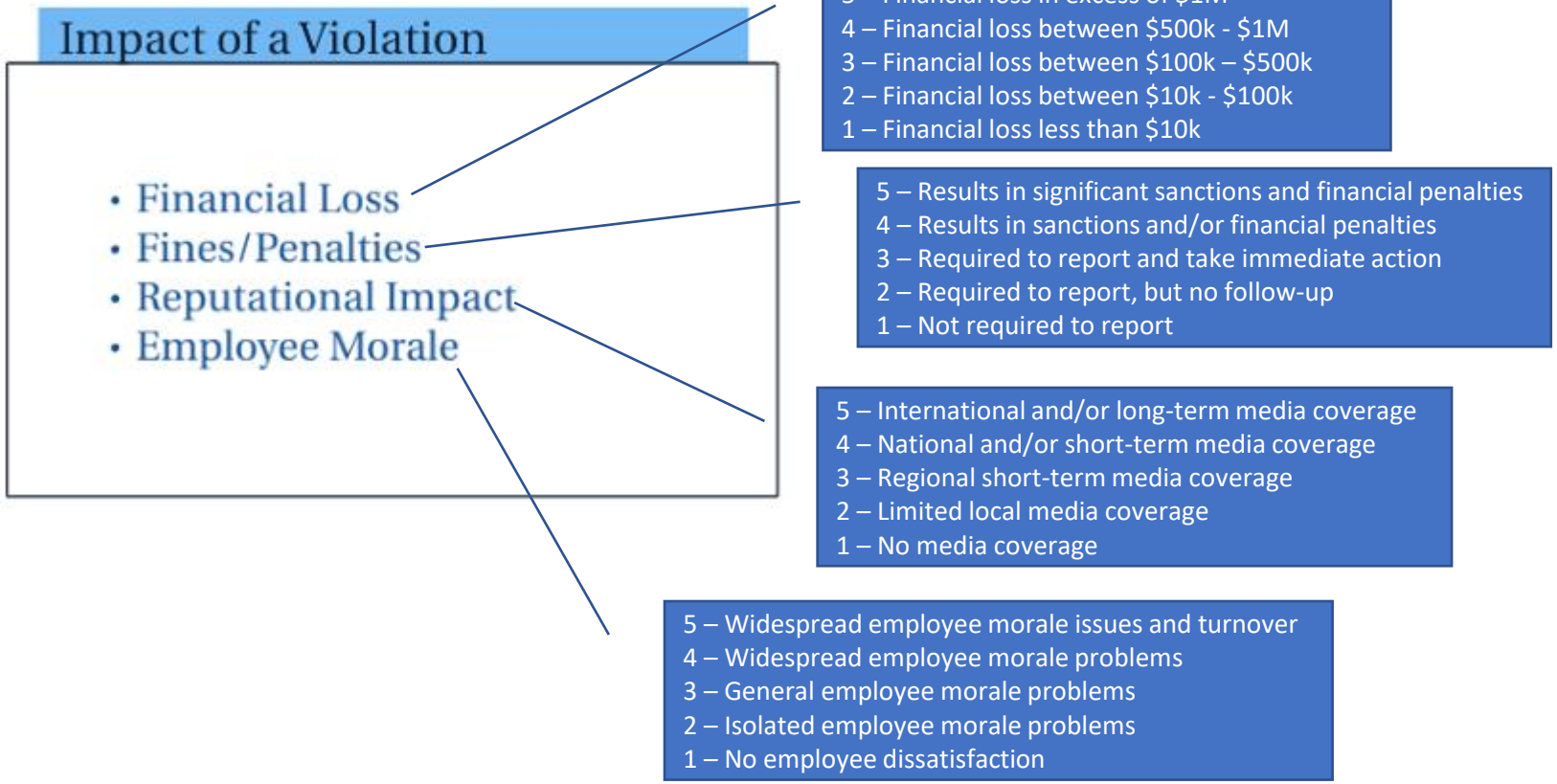


The risk of Cash Larceny:

- Receive cash daily (5)
- Reasonably possible (3)
- Simple and easy to commit (5)

- Average Likelihood score = 4.3

Assess the Impact

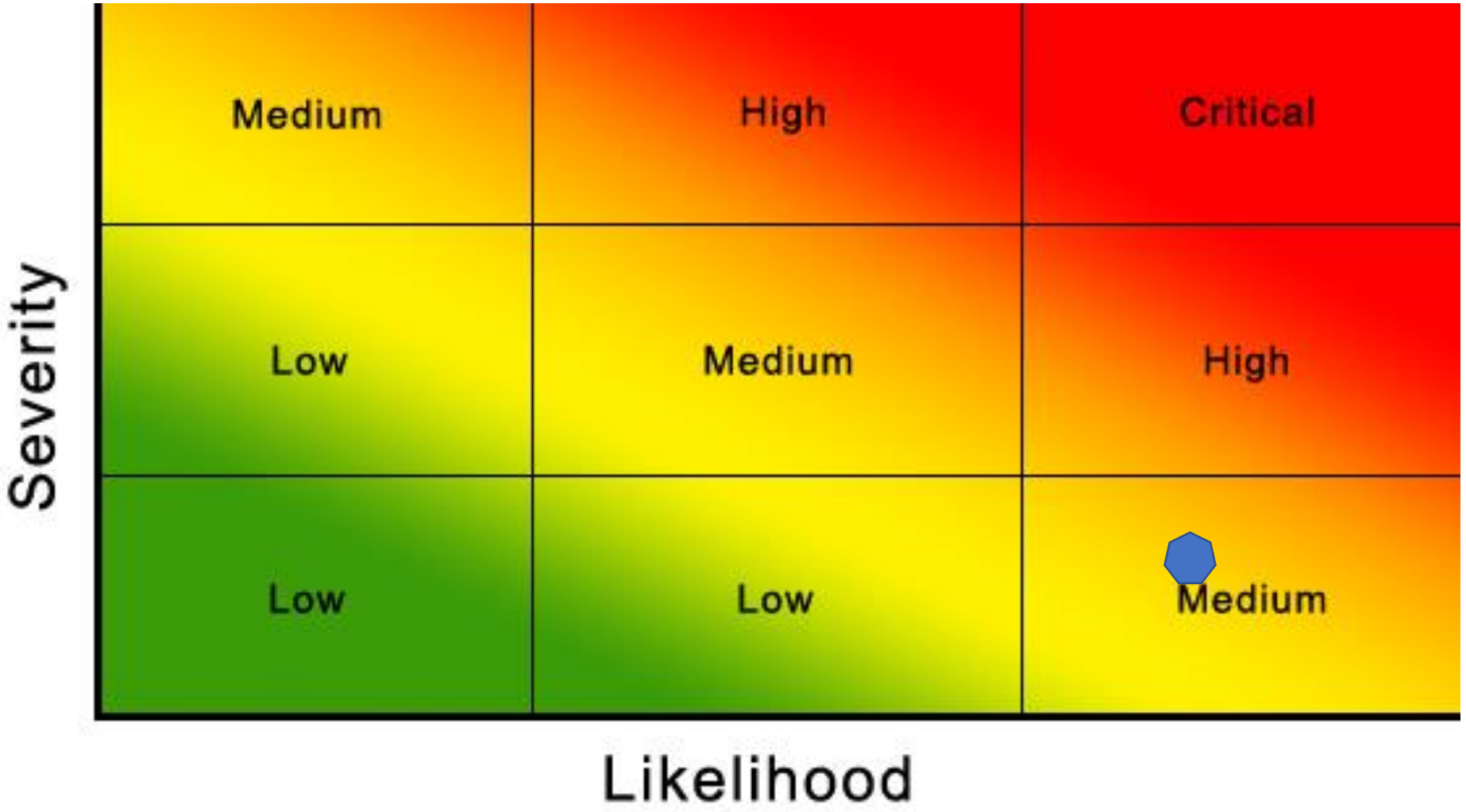


The risk of Cash Larceny:

- Cash available to employee is limited / small (1)
- Not required to report small thefts (1)
- Limited local media coverage at most if at higher scale (2)
- Isolated morale issues if others know it's happening, and nothing is done (2)

- Average Impact score = 1.5

Compliance Risk Heat Map – Inherent Risk



Compliance Risk Assessment Scorecard

Program Element	Green	Yellow	Red
Oversight	The program has a clear owner that provides reports on a regular basis to the Office of the Chief Compliance Officer	The program has an owner, but does not provide reports to the Office of the Chief Compliance Officer	The program does not have a clear owner
Due Diligence / Communication	Background check is conducted on all employees' time of hire in accordance with company's employment requirements. Relevant employees receive additional screening at time of internal transfer or promotion to confirm background screen and review of existing personnel file and Ethics Line database; review does not indicate that individual hired/promoted has engaged in illegal conduct or other conduct that is inconsistent with an effective compliance program.	Background check is conducted at time of hire but not at time of internal transfer from a non-relevant role to a relevant role or at the time of promotion within relevant roles.	Background checks have not been conducted for all new hires, internal transfers, and promotions, are performed using inconsistent standards between hiring locations, or negative background results are ignored
Disciplinary Action	The policy clearly states that all employees found to be intentionally non-compliant are disciplined or separated, and all employees found to be unknowingly non-compliant are disciplined or retrained.	The policy is in place, but some employees found to be non-compliant have not been adequately disciplined.	There is no policy in place regarding enforcement and discipline due to non-compliance.
Risk Assessment	Yes. A risk assessment has been completed specifically around this topic area in the past 2 years	Yes. This topic area has been included in a general compliance risk assessment that has been completed in the past 2 years	No. A risk assessment has not been completed in over 2 years
Auditing	The compliance program has been audited by an independent audit function, such as Internal Audit within the last year	The compliance program has been audited by an independent audit function, such as Internal Audit within the past two years	The compliance program has not been audited by an independent audit function in over two years.
	No non-conformances/issues were detected through audits	Less than 5 minor non-conformances to legal requirements	One or more major non-conformances to legal requirements
Enforcement Actions	0 investigations/charges per year	1 investigation/charge per year	More than 1 investigation/charge per year
	There are no damages, settlements, or fines from litigation due to compliance failures	Total damages, settlements, and fines from litigation due to compliance failures is within 5% (+ or -) of target	Total damages, settlements, and fines from litigation due to compliance failures is greater than 5% (+ or -) of target
	There are no new lawsuits filed against the company/open litigation matters	Number of new lawsuits filed against the company/open litigation matters is within 5% (+ or -) of target	Number of new lawsuits filed against the company/open litigation matters is greater than 5% (+ or -) of target

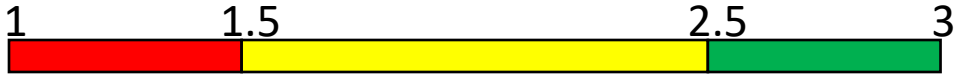
Compliance Risk Assessment Scorecard

Program Element	Green	Yellow	Red
Standards & Procedures	The policy/M&Ps are in place and have been reviewed in the past year	The policy/M&Ps are in place, but have not been reviewed in over a year	No corporate policy/M&Ps exists
	The policy/M&Ps are available to 100% of relevant employees	Greater than 90% of relevant employees have read and understand the policy/M&Ps	The M&Ps are not available to all relevant employees or less than 90% of employees have read and understand the policy
Training & Education	Trainings are mandatory and available to all relevant employees for understanding all relevant compliance laws	Yes, trainings are available, but are not mandatory and/or are not in a format that will reach all relevant employees	No, trainings are not available
	100% of relevant employees complete the available training courses	Greater than 90% of relevant employees complete the available training courses	Less than 90% of relevant employees complete the available training courses
Monitoring	There is a process in place to regularly (more than once a year) internally monitor compliance with applicable laws	The compliance program has been internally monitored within the last year	There is no current monitoring being conducted
	No non-conformances/issues were detected through audits	Less than 5 minor non-conformances to legal requirements	One or more major non-conformances to legal requirements
Corrective Action	The spending level on compliance activities is within budget	The spending level on compliance activities is within 5% (+ or -) of budget	The spending level on compliance activities is greater than 5% (+ or -) of budget
	Less than 90 days	Between 90 and 120 days	Greater than 120 days

Compliance Summary Scorecard

	Program Element								
Compliance Area	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Area Total**
Fraud - Larceny									**2.68**

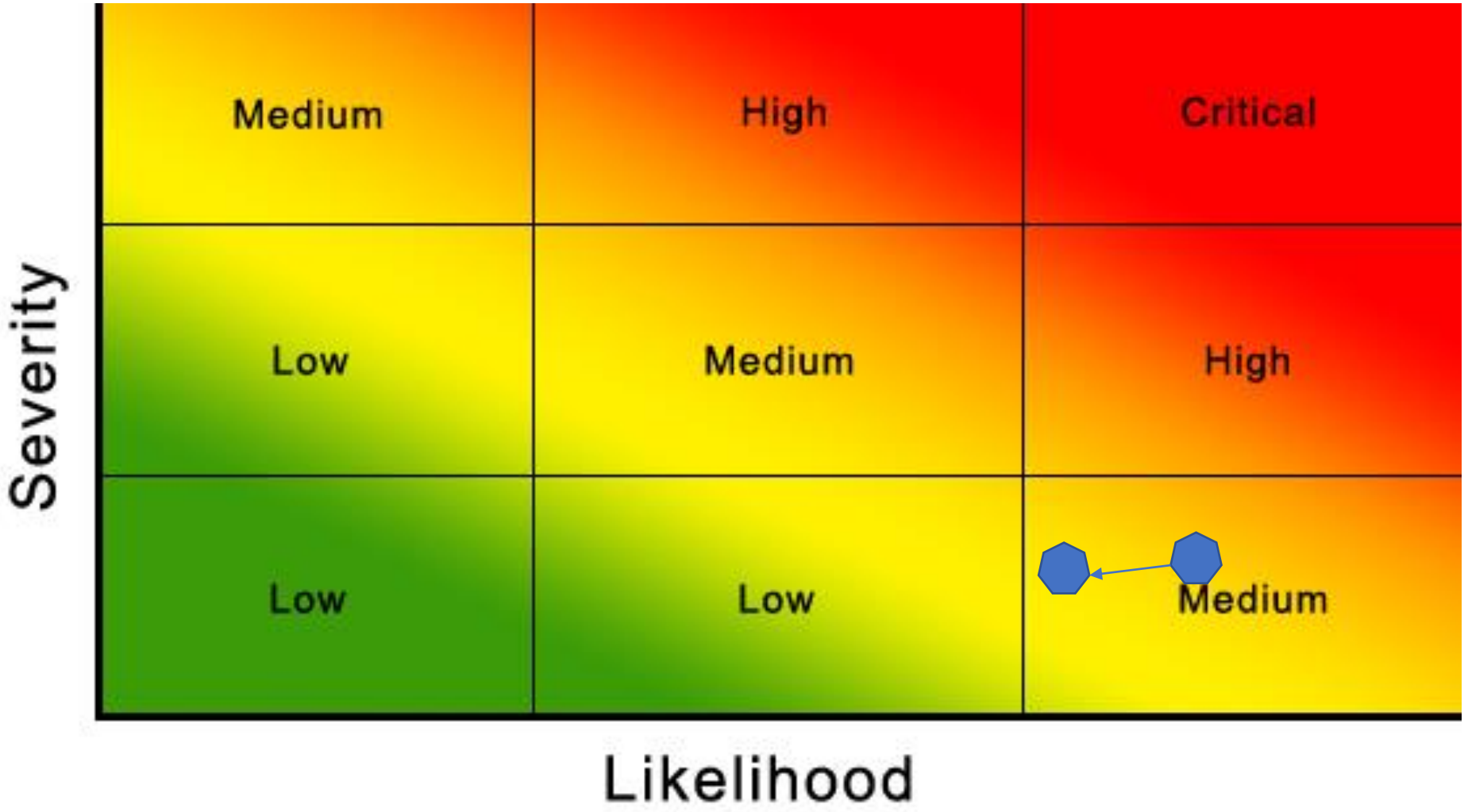
Rating Scale:



1 - Standards and Procedures
2 - Oversight - Compliance Officer or Compliance Committee
3 - Due Diligence/Open Lines of Communication
4 - Training and Education

5 - Auditing and Monitoring
6 - Enforcement and Disciplinary
7 - Corrective Action Procedures (Response and Prevention)
8 – Risk Assessment

Compliance Risk Heat Map – Inherent Risk



Ethical Considerations

- Remote from Manager
- Manage Has Large Span of Control
- Top Performer
- ✓Marginal Performer
- Third Party Selection / Assessment
- Vendor / Counterparty / Due Diligence
- Regulated Activity
- Overseas Market
- High Risk Market
- Signing Authority and Level
- Market Share
- Objectivity required
- Deals with Politically Exposed Persons (PEPs)

Ethical Considerations

- Number of alerts generated for policy violations (Travel & Expense; Employee Fraud; Harassment/Discrimination; Bribery, Corruption & Insider Trading; Customer and Vendor Complaints; etc.)

✓ Number of Hotline complaints

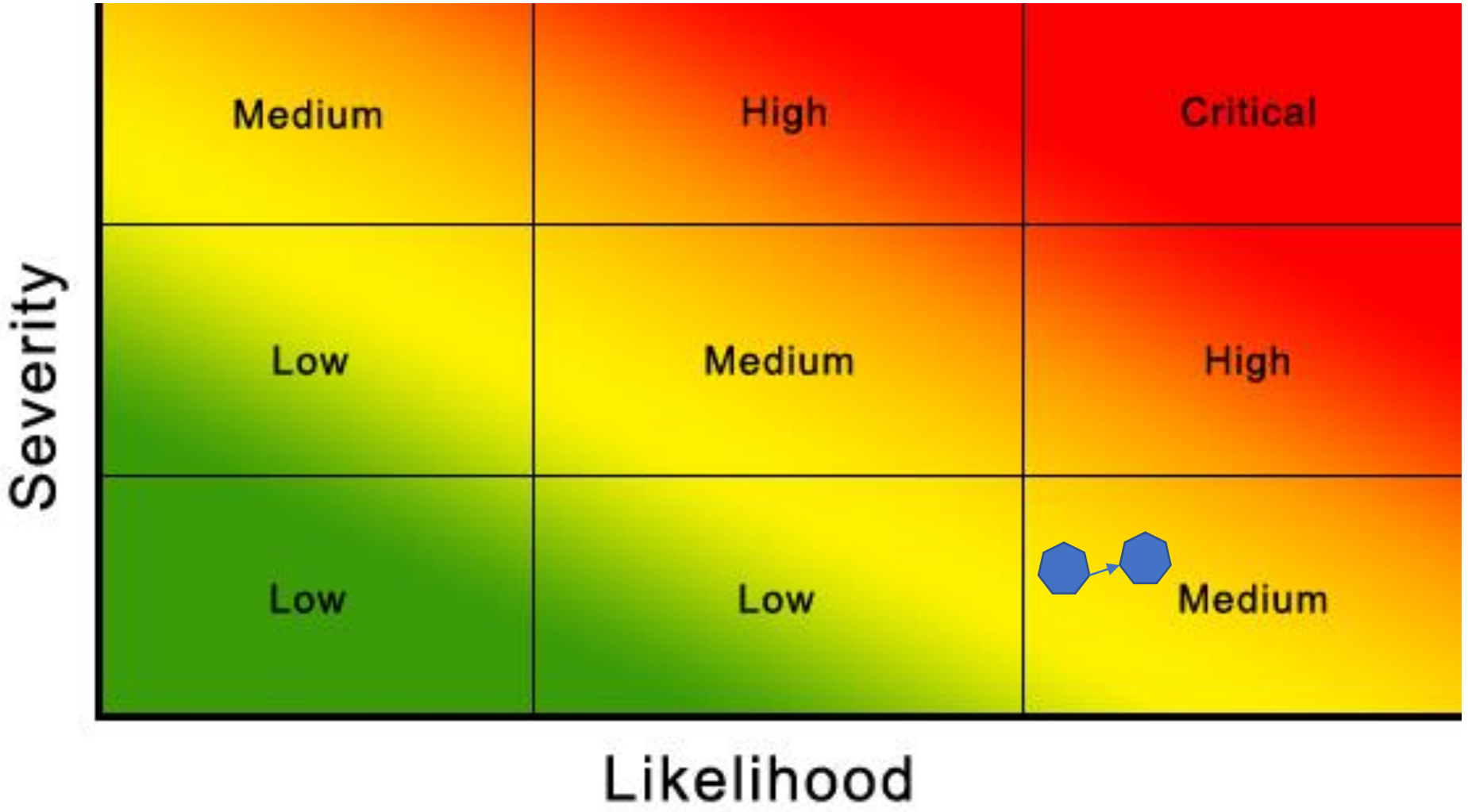
✓ Training statistics (promptness in taking mandatory training, question-level analysis of success rates, level of participation in non-mandatory training)

✓ Assess across units (what culture problems do you have and where do you have them)

  - Certain business functions and job categories present a higher level of risk in terms of ethical behavior – **Sales**; Vendor Management; Trading; etc.

- Focus on level of seniority – Are they leading by example?

Compliance Risk Heat Map – Inherent Risk



Other Controls

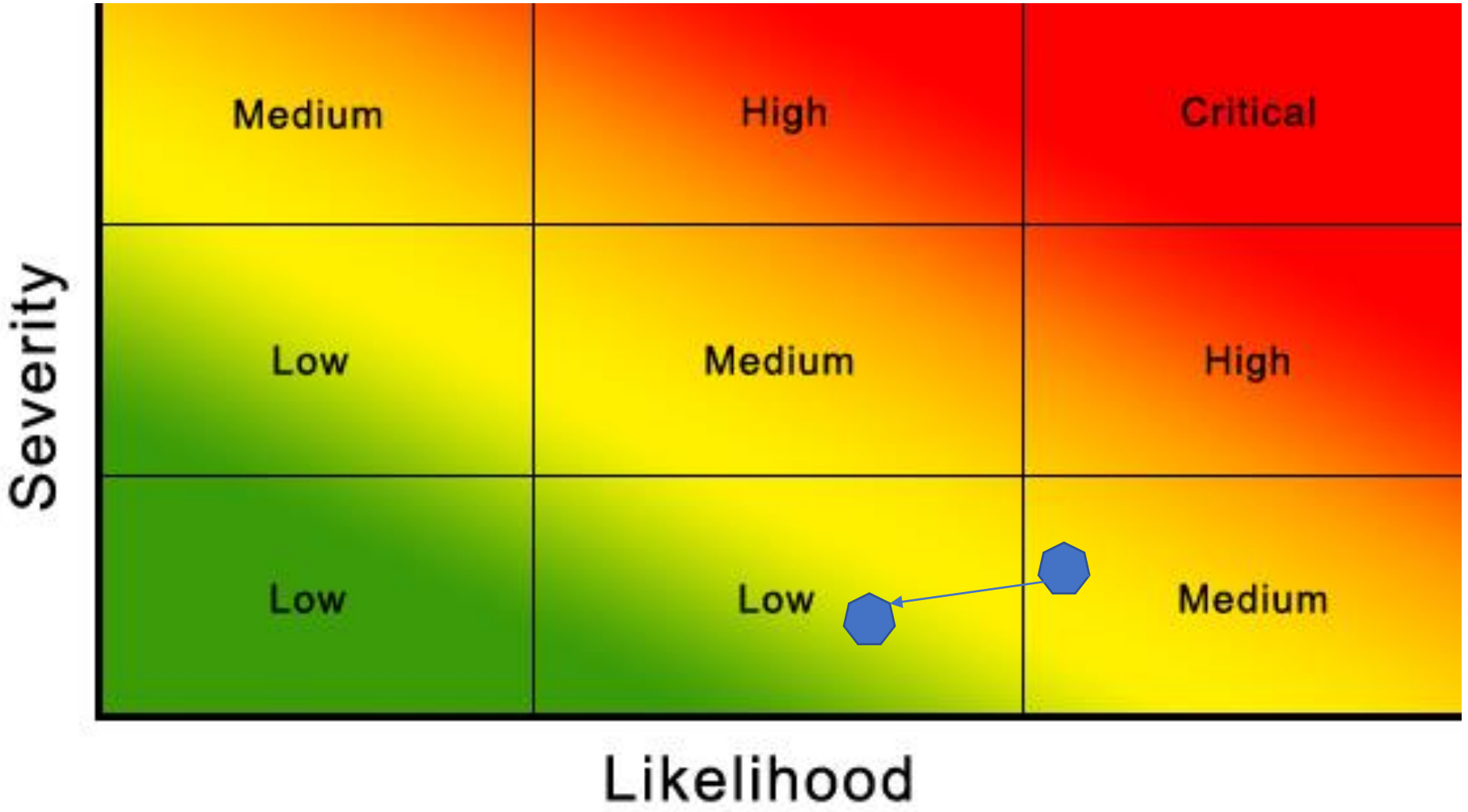
- Review/count of register each evening
- Monthly trend report for missing money
- Security cameras in stores
- Second person makes deposits
- Money kept in safe after register is counted

Reduce Likelihood for effective controls.

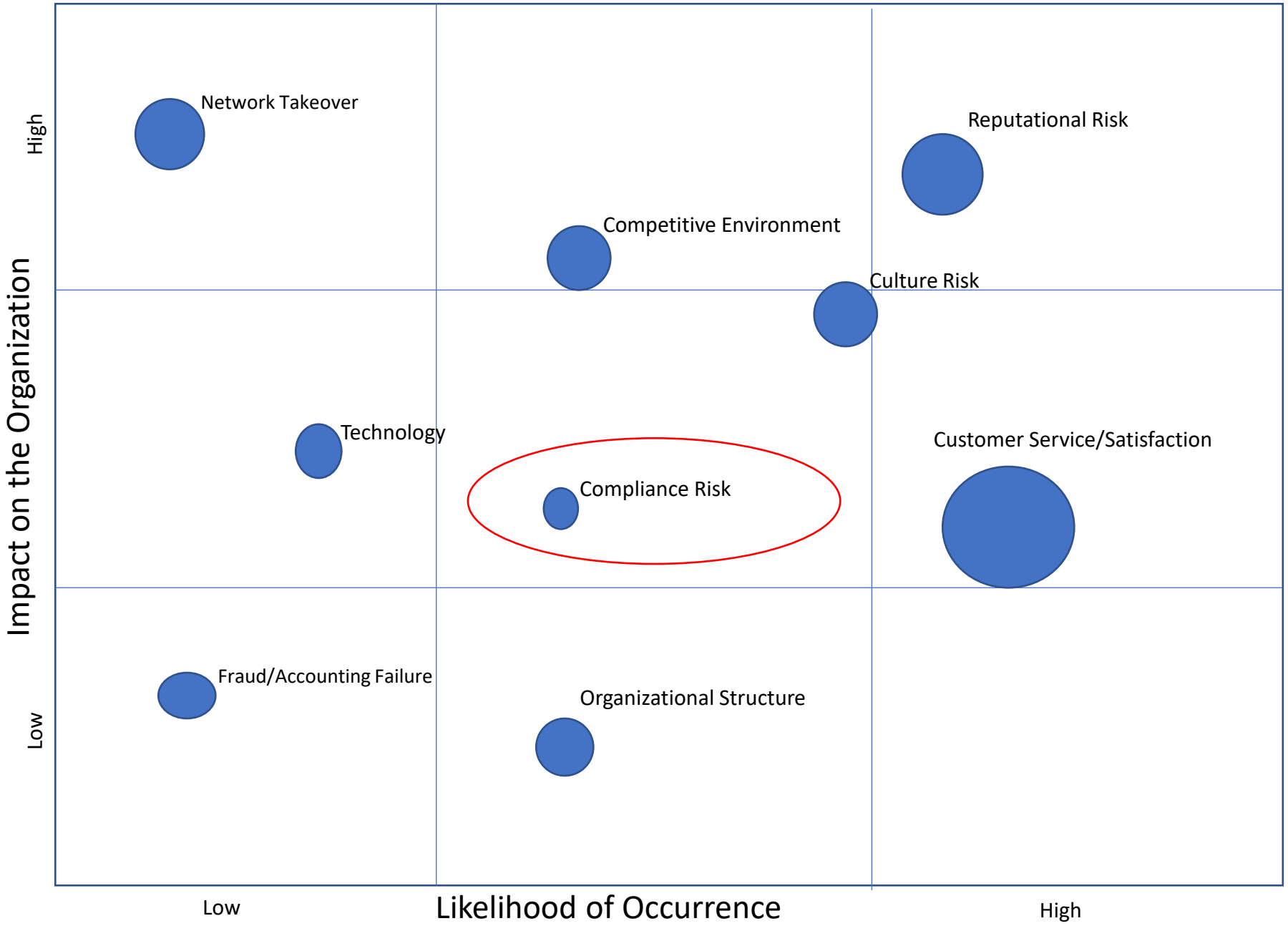
- Insurance Policy for Employee Fraud

Reduce Impact for effective control.

Compliance Risk Heat Map – Residual Risk



Enterprise Risk Management Model

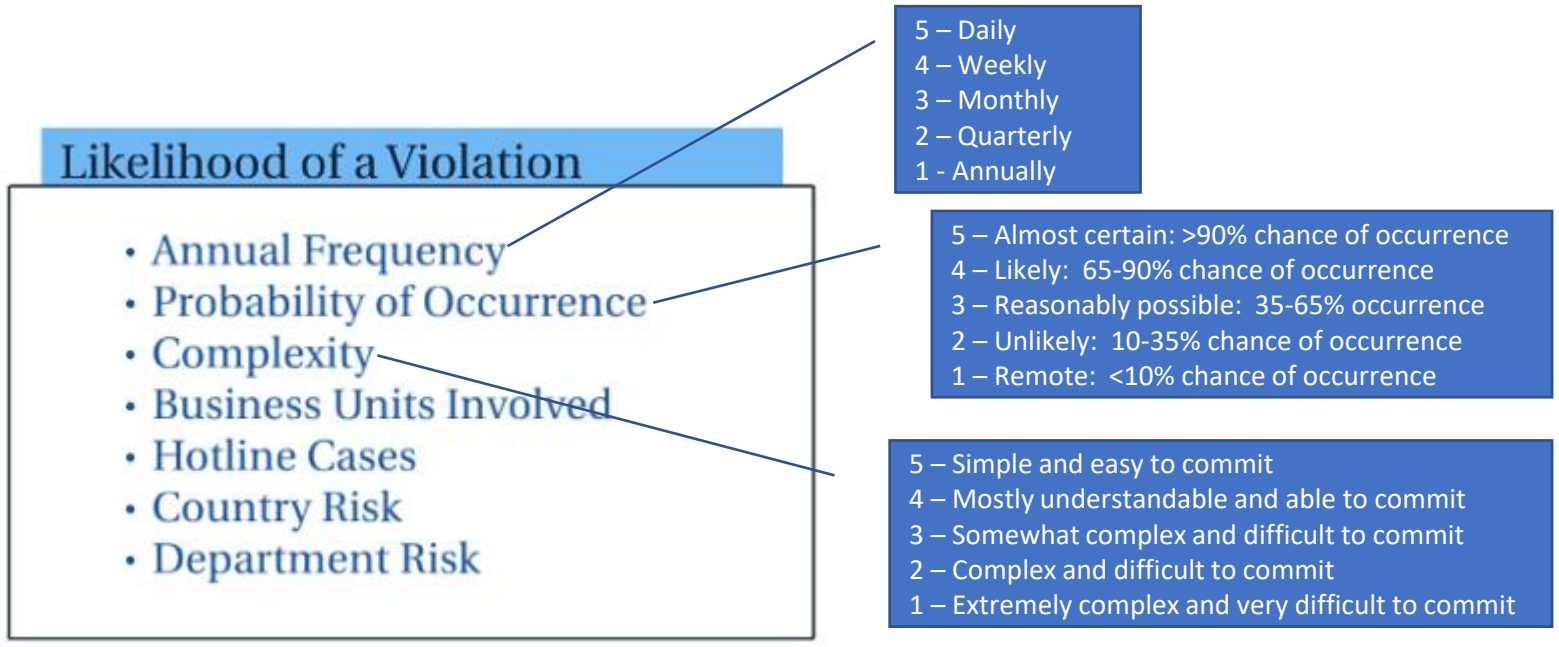


Example Cyber-related Compliance Risks

Risk Level 1	Risk Description
Cybersecurity / Information Security Breach	The risk that the company's information technology does not have adequate controls and allows for threats such as hacking, data breaches, security incidents, etc.
Privacy Regulations	The risk of the company not adhering to the regulations applicable to the company
Receipt and Handling of PII	The risk that the company does not properly handle resident, vendor, or team member PII, resulting in a loss or breach of the data.
Data Governance	The risk that the company does not have the proper governance (availability, usability, and security) of the data in its enterprise systems to ensure that data is consistent, trustworthy and not misused.

Assess the Likelihood

Risk Description: The risk that the company's information technology does not have adequate controls and allows for threats such as hacking, data breaches, security incidents, etc.

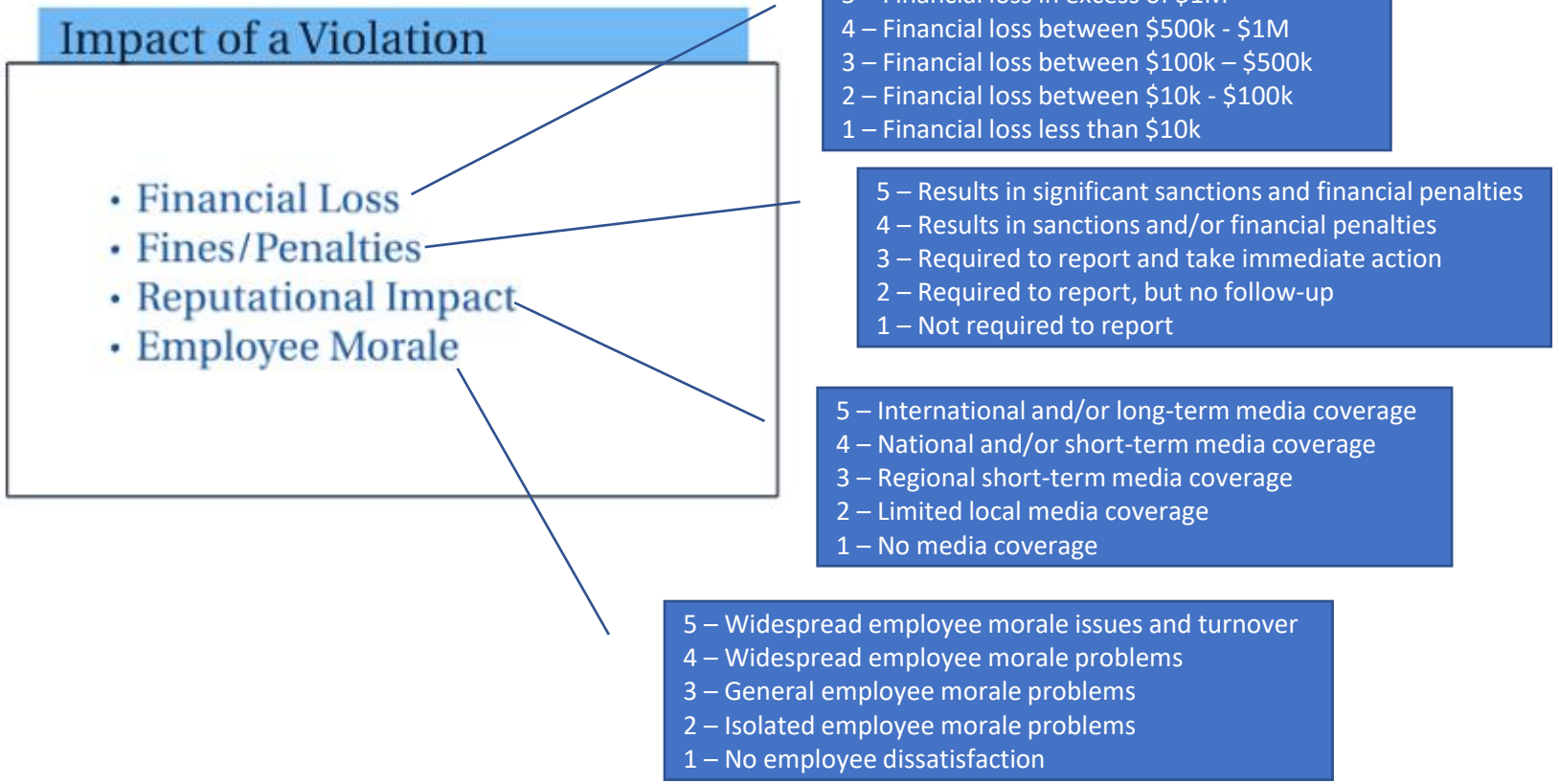


The risk of Cybersecurity / Information Security Breaches

- Use systems daily / receive threats daily (5)
- Almost certain (5)
- Mostly understandable and able to commit (4)

- Average Likelihood score = 4.7

Assess the Impact

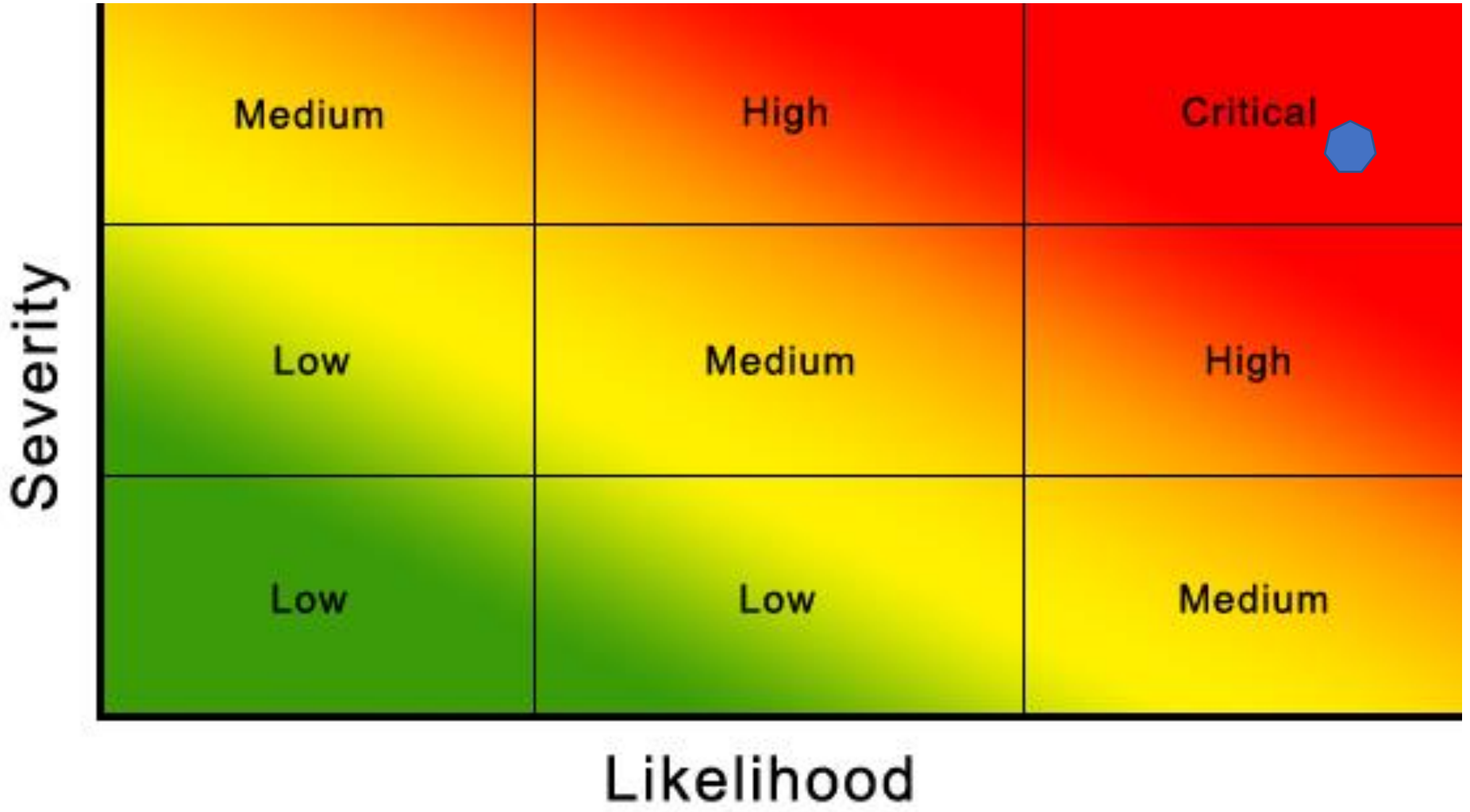


The risk of Cybersecurity / Information Security Breaches.

- Huge financial loss if systems down or if theft of information (5)
- Data breach requirements by state (5)
- If major breach, could impact media coverage, depending on response (4)
- Could result in general employee morale issues and questions about company continuity (3)

- Average Impact score = 4.3

Compliance Risk Heat Map – Inherent Risk



Compliance Risk Assessment Scorecard

Program Element	Green	Yellow	Red
Oversight	The program has a clear owner that provides reports on a regular basis to the Office of the Chief Compliance Officer	The program has an owner, but does not provide reports to the Office of the Chief Compliance Officer	The program does not have a clear owner
Due Diligence / Communication	Background check is conducted on all employees' time of hire in accordance with company's employment requirements. Relevant employees receive additional screening at time of internal transfer or promotion to confirm background screen and review of existing personnel file and Ethics Line database; review does not indicate that individual hired/promoted has engaged in illegal conduct or other conduct that is inconsistent with an effective compliance program.	Background check is conducted at time of hire but not at time of internal transfer from a non-relevant role to a relevant role or at the time of promotion within relevant roles.	Background checks have not been conducted for all new hires, internal transfers, and promotions, are performed using inconsistent standards between hiring locations, or negative background results are ignored
Disciplinary Action	The policy clearly states that all employees found to be intentionally non-compliant are disciplined or separated, and all employees found to be unknowingly non-compliant are disciplined or retrained.	The policy is in place, but some employees found to be non-compliant have not been adequately disciplined.	There is no policy in place regarding enforcement and discipline due to non-compliance.
Risk Assessment	Yes. A risk assessment has been completed specifically around this topic area in the past 2 years	Yes. This topic area has been included in a general compliance risk assessment that has been completed in the past 2 years	No. A risk assessment has not been completed in over 2 years
Auditing	The compliance program has been audited by an independent audit function, such as Internal Audit within the last year	The compliance program has been audited by an independent audit function, such as Internal Audit within the past two years	The compliance program has not been audited by an independent audit function in over two years.
	No non-conformances/issues were detected through audits	Less than 5 minor non-conformances to legal requirements	One or more major non-conformances to legal requirements
Enforcement Actions	0 investigations/charges per year	1 investigation/charge per year	More than 1 investigation/charge per year
	There are no damages, settlements, or fines from litigation due to compliance failures	Total damages, settlements, and fines from litigation due to compliance failures is within 5% (+ or -) of target	Total damages, settlements, and fines from litigation due to compliance failures is greater than 5% (+ or -) of target
	There are no new lawsuits filed against the company/open litigation matters	Number of new lawsuits filed against the company/open litigation matters is within 5% (+ or -) of target	Number of new lawsuits filed against the company/open litigation matters is greater than 5% (+ or -) of target

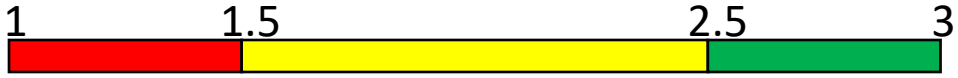
Compliance Risk Assessment Scorecard

Program Element	Green	Yellow	Red
Standards & Procedures	The policy/M&Ps are in place and have been reviewed in the past year	The policy/M&Ps are in place, but have not been reviewed in over a year	No corporate policy/M&Ps exists
	The policy/M&Ps are available to 100% of relevant employees	Greater than 90% of relevant employees have read and understand the policy/M&Ps	The M&Ps are not available to all relevant employees or less than 90% of employees have read and understand the policy
Training & Education	Trainings are mandatory and available to all relevant employees for understanding all relevant compliance laws	Yes, trainings are available, but are not mandatory and/or are not in a format that will reach all relevant employees	No, trainings are not available
	100% of relevant employees complete the available training courses	Greater than 90% of relevant employees complete the available training courses	Less than 90% of relevant employees complete the available training courses
Monitoring	There is a process in place to regularly (more than once a year) internally monitor compliance with applicable laws	The compliance program has been internally monitored within the last year	There is no current monitoring being conducted
	No non-conformances/issues were detected through audits	Less than 5 minor non-conformances to legal requirements	One or more major non-conformances to legal requirements
Corrective Action	The spending level on compliance activities is within budget	The spending level on compliance activities is within 5% (+ or -) of budget	The spending level on compliance activities is greater than 5% (+ or -) of budget
	Less than 90 days	Between 90 and 120 days	Greater than 120 days

Compliance Summary Scorecard

	Program Element								
Compliance Area	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Area Total**
Fraud - Larceny									**2.81**

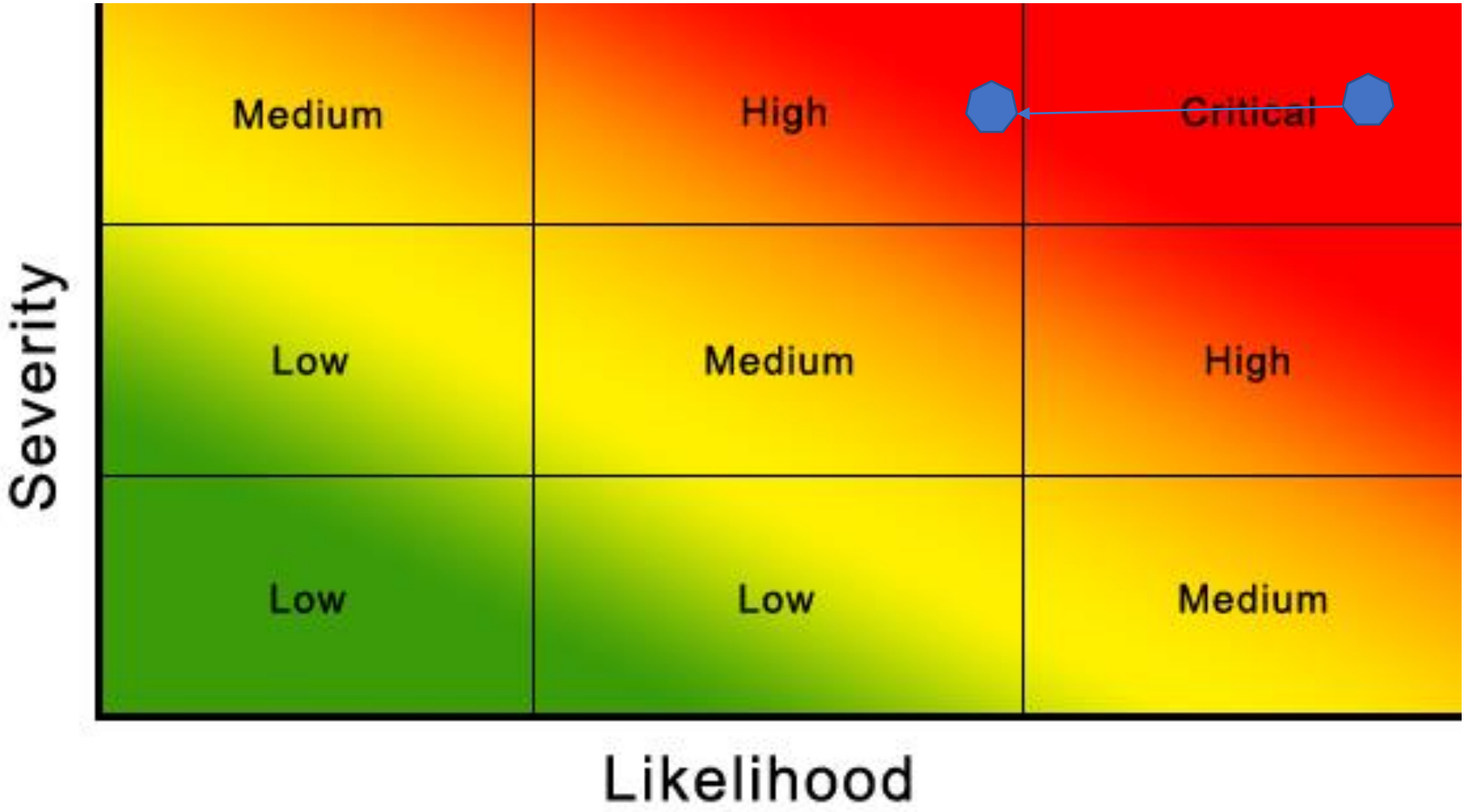
Rating Scale:



1 - Standards and Procedures
2 - Oversight - Compliance Officer or Compliance Committee
3 - Due Diligence/Open Lines of Communication
4 - Training and Education

5 - Auditing and Monitoring
6 - Enforcement and Disciplinary
7 - Corrective Action Procedures (Response and Prevention)
8 – Risk Assessment

Compliance Risk Heat Map – Inherent Risk



Ethical Considerations

- ✓Remote from Manager
- Manage Has Large Span of Control
- Top Performer
- Marginal Performer
- ✓Third Party Selection / Assessment
- ✓Vendor / Counterparty / Due Diligence
- Regulated Activity
- ✓Overseas Market
- High Risk Market
- Signing Authority and Level
- Market Share
- Objectivity required
- Deals with Politically Exposed Persons (PEPs)

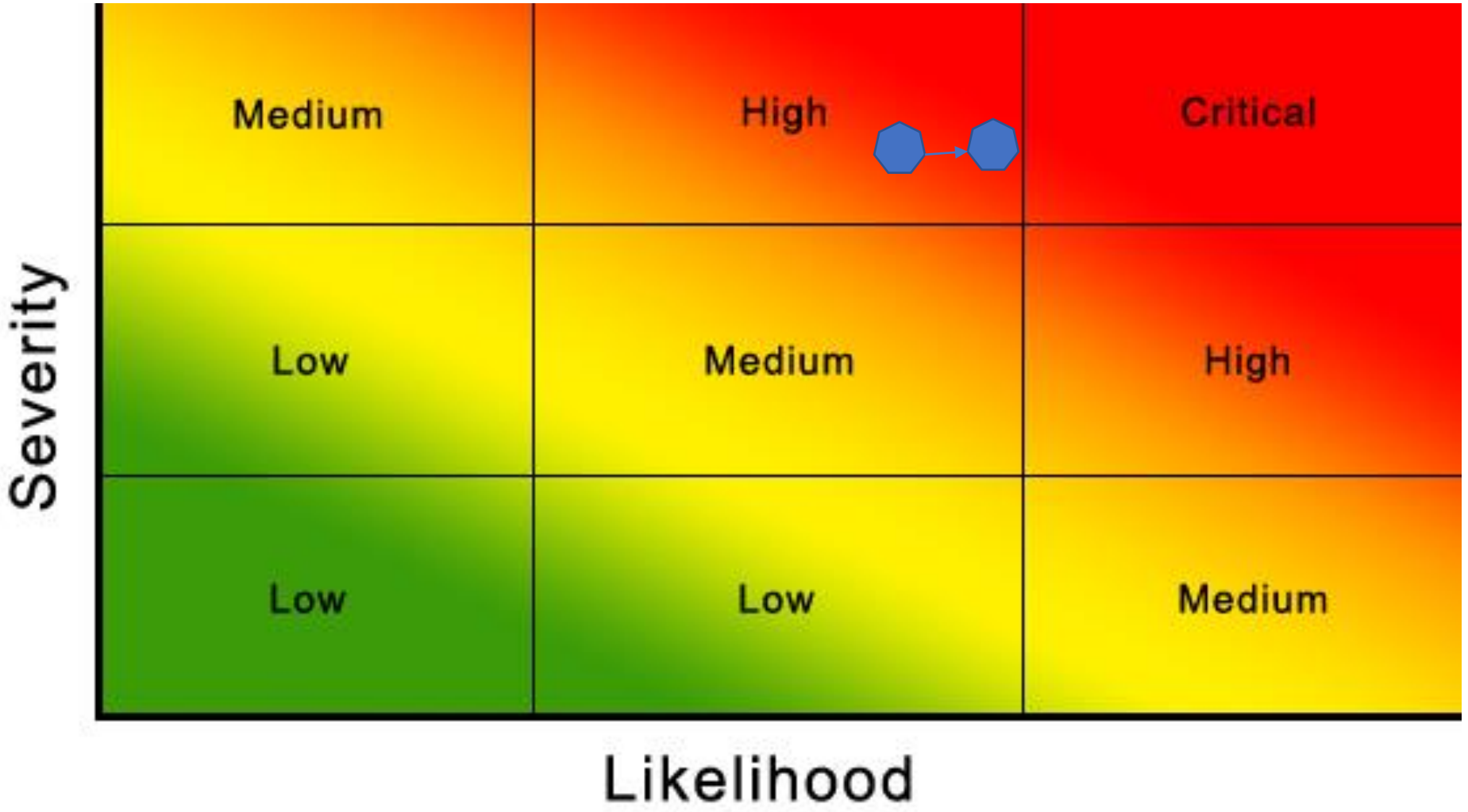
Ethical Considerations

- Number of alerts generated for policy violations (Travel & Expense; Employee Fraud; Harassment/Discrimination; Bribery, Corruption & Insider Trading; Customer and Vendor Complaints; etc.)
- Number of Hotline complaints

✓Training statistics (promptness in taking mandatory training, question-level analysis of success rates, level of participation in non-mandatory training)

- Assess across units (what culture problems do you have and where do you have them)
    - Certain business functions and job categories present a higher level of risk in terms of ethical behavior – Sales; Vendor Management; Trading; etc.
- Focus on level of seniority – Are they leading by example?

Compliance Risk Heat Map – Inherent Risk



Other Controls

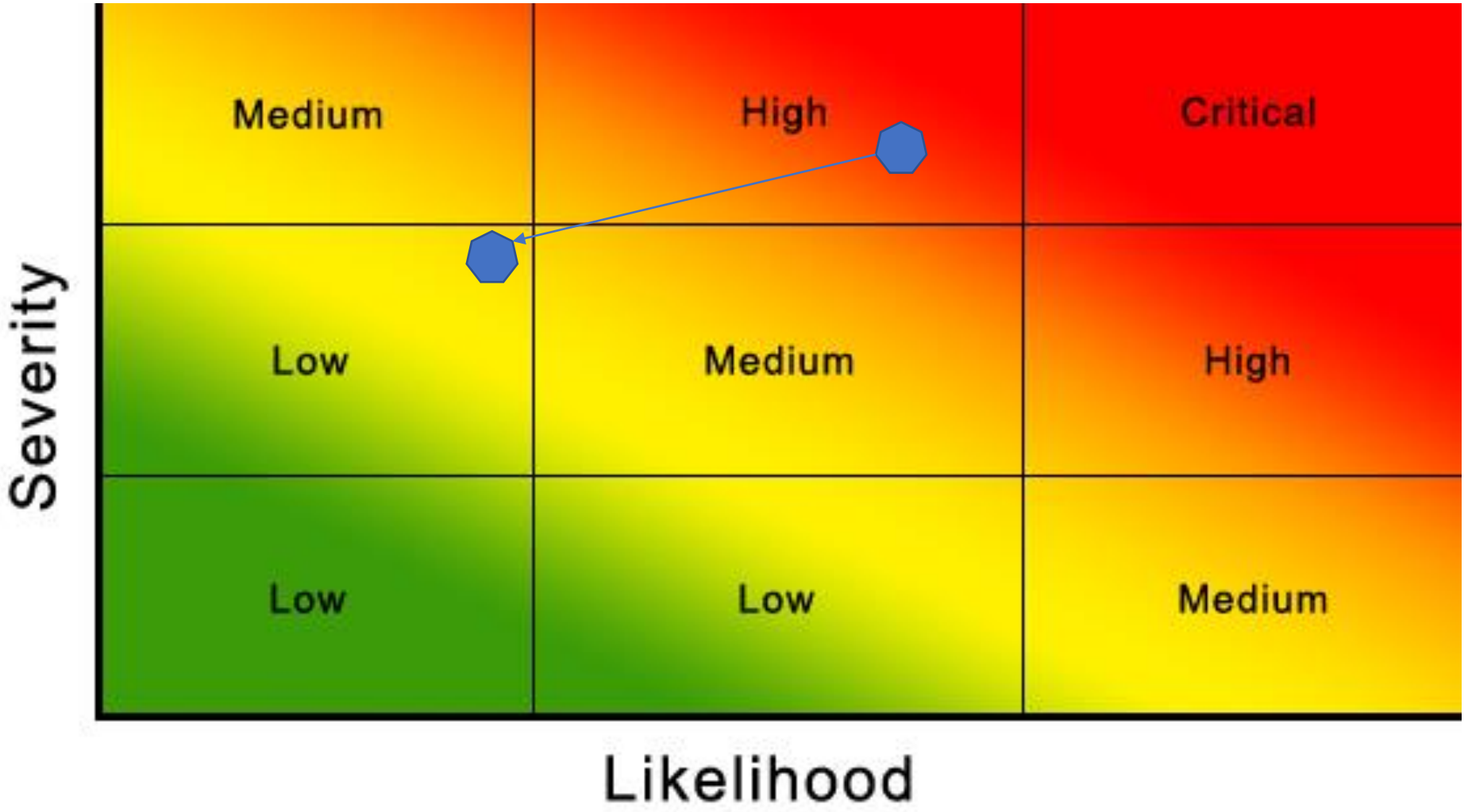
- Penetration testing
- Review of access controls
- Vendor security reviews at onboarding
- Reduction of number of admin accounts

Reduce Likelihood for effective controls.

- Cyber Insurance policy

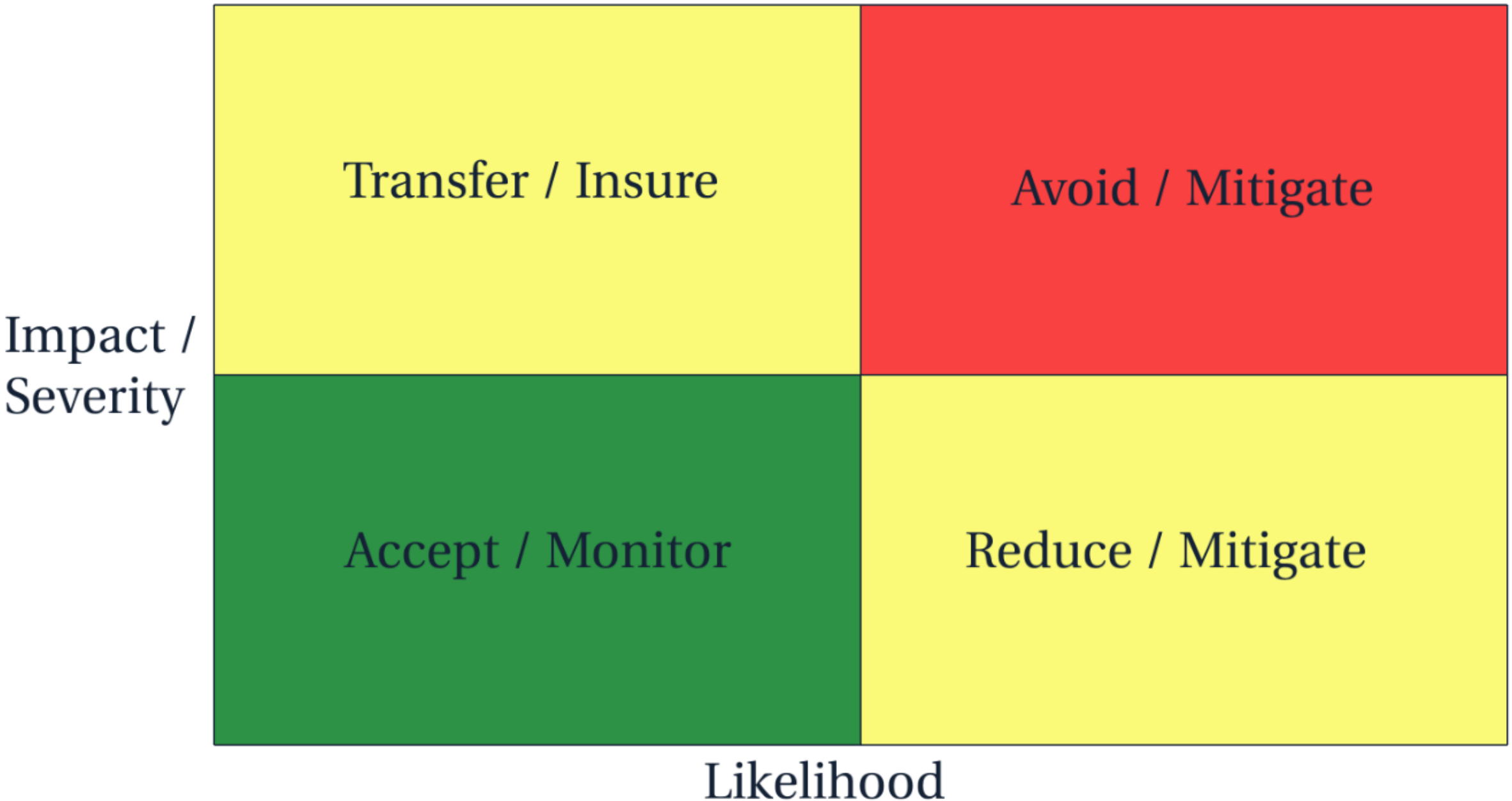
Reduce Impact for effective control.

Compliance Risk Heat Map – Residual Risk



So What? Now What?

Manage/Treat the Risk



An Ethical Culture Leads Employees to Do the Right Thing

- Proper Enterprise Risk Assessments, which incorporate compliance and ethics, can lead to identification of areas where management should spend the most resources

- Hotline reporting rates increase when the company has:
  - An effective compliance program
  - A strong ethical culture
  - Both top and middle management that are committed to ethics
  - The same standard for misconduct by all levels of employees in the company
  - Only isolated incidents of misconduct instead of pervasive, company-wide misconduct

Questions?

ELIZABETH SIMON
VP, COMPLIANCE
FIRSTKEY HOMES