ALL ABOUT YOU!

8TH ANNUAL PERSPECTIVE USERS' CONFERENCE
MARCH 1-2 , 2016

PERSPECTIVE:
powered by RESOLVER

Risk-Incidents: Same Playground, Different Castles

Brian C. McIlravey

Fi

Risk & Incidents: Same Sand – Different Castles

Risk & Incidents: Same Sand, Same Castles: Different Properties

RISK!

Likelihood!

Impact?

AT YOUR OWN RISK

LOW RISK
HIGH RISK
NO RISK

RISK
REWARD

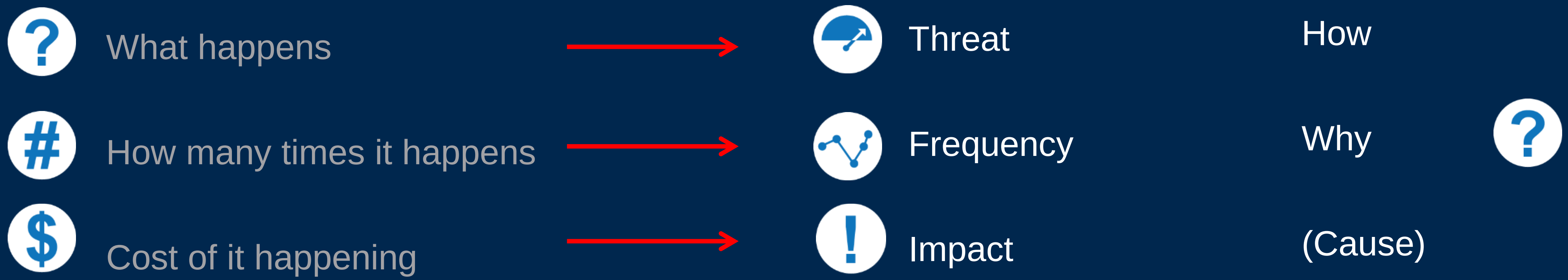
RISK

AVOID
REDUCE
RISK
SFER

RISK
MANAGEMENT
IDENTIFICATION
PROCESS
PROBABILITY
PROJECT
LOSS
INFORMATION
ASSESSMENT
COST
BUSINESS
EVENT
INSURANCE
IMPACT
COMMUNICATION
RESOURCES
MITIGATION
ANALYSIS
DEVELOPMENT
OCCURRENCE
CONSEQUENCES
IMPLEMENTATION
ORGANIZATION
FINANCIAL
COMPANY
POSSIBLE
EVENTS
SECURITY
PARTICULAR
VALUE
REDUCTION
POTENTIAL
CONTROL
CONTROLS
DECISIONS
PRACTICE
TIME
TERMS
FOLLOWING
ACTIVITIES
SCHEDULE
IDENTIFIED
ASSESSED
CAUSE
SOURCES
SOURCE
MANAGING
BASED
APPLIED
NEGATIVE
HIGH
PLAN
TECHNOLOGY
METHOD
MEASURES
THREATS
ENTERPRISE
AVAILABLE
HAZARD
SEVERAL
TRANSFER
PROBLEM
FORMULA
AVOID
SOFTWARE
EFFECTIVE
PREVENTION
OCCUR
CASE
COMPOSITE
PLANNING
OPERATIONAL
PROCESSES
MARKET
SAFETY
THREAT
OBJECTIVES
CONTEXT
KNOWN
GROUP
EXTERNAL
DIAGRAMS
SIMPLY
POLICY
MOST
TIE
DEFINED
UNCERTAINTY
STANDARD
INTERNATIONAL
DECISION
ACCEPT
HANDLED
KNOWLEDGE
LIABILITY
TAXONOMY
DIFFERENT
PLANS
ASSETS
ACCEPTED
APPROPRIATE
SPECIFIC
INCREASE
RELATED
OCCURS
LOSSES
WASTE
AREAS
TAKE
OCCURRING
MAIN
LEVEL
EFFECT
BENEFIT
TERM

Risk Management: The Primary Function of Security

Assess, manage and mitigate risk… using existing information.



What happens → Threat

How many times it happens → Frequency

Cost of it happening → Impact

How

Why

(Cause)

What We Know About Incidents

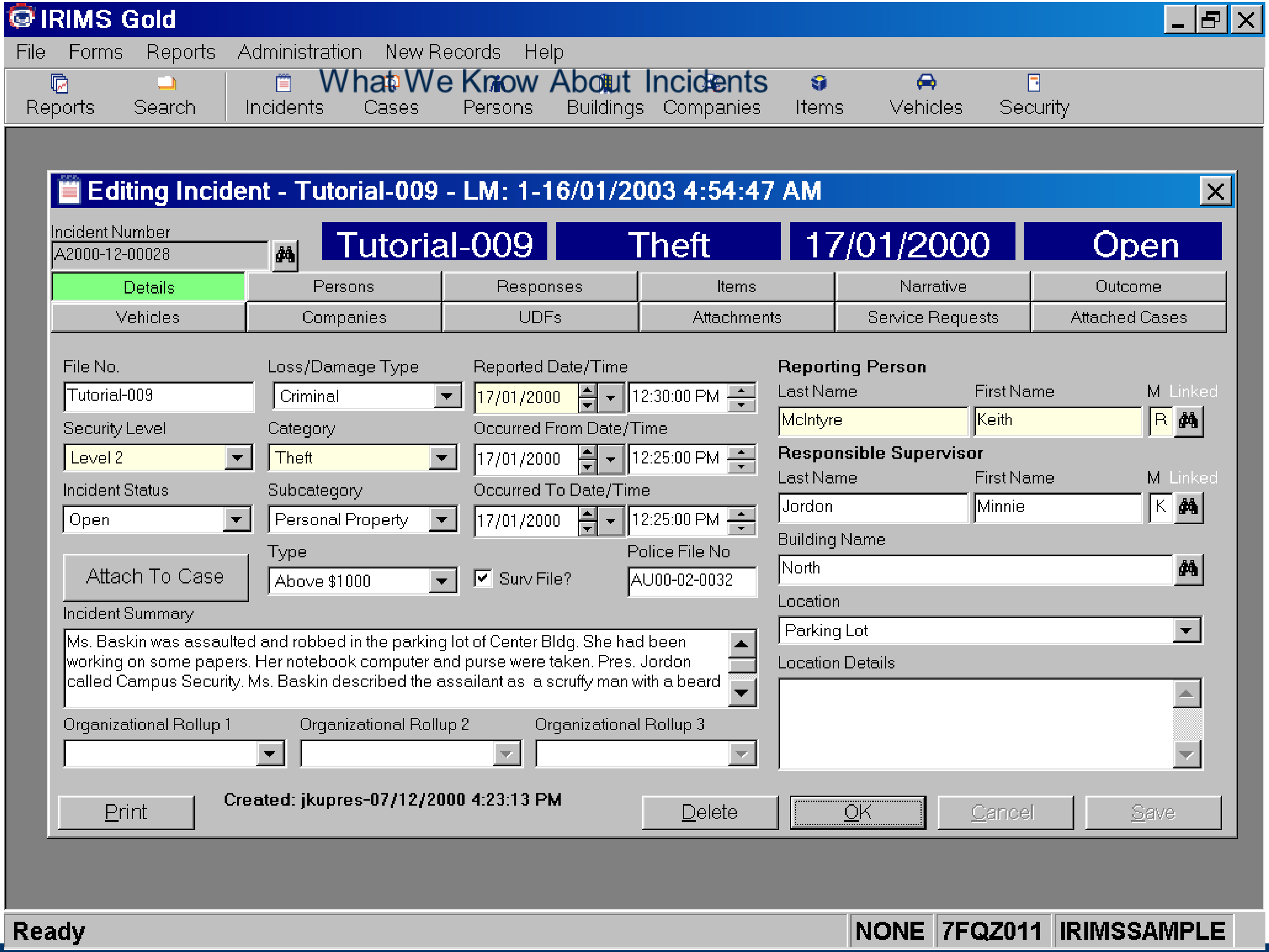
Incident Types

Natural Events	Human Driven Events	Uncontrolled Events
Tornados	Thefts	Fires/Explosions
Hurricanes	Assaults	Surrounded Event
Storms	Murders	Personal Injury Accidents
Floods	Bombs	Industrial Accidents
Earthquakes	Frauds	System Failures

IT HR Risk Management Legal Security Ethics Compliance Safety Environment

Incidents and Events at Departmental Level

What We Know About Incidents



Editing Incident - Tutorial-009 - LM: 1-16/01/2003 4:54:47 AM

Incident Number: A2000-12-00028

Tutorial-009 | Theft | 17/01/2000 | Open

File No.: Tutorial-009

Loss/Damage Type: Criminal

Reported Date/Time: 17/01/2000 12:30:00 PM

Security Level: Level 2

Category: Theft

Occurred From Date/Time: 17/01/2000 12:25:00 PM

Incident Status: Open

Subcategory: Personal Property

Occurred To Date/Time: 17/01/2000 12:25:00 PM

Type: Above $1000

☑ Surv File?

Police File No: AU00-02-0032

Incident Summary: Ms. Baskin was assaulted and robbed in the parking lot of Center Bldg. She had been working on some papers. Her notebook computer and purse were taken. Pres. Jordon called Campus Security. Ms. Baskin described the assailant as a scruffy man with a beard

Organizational Rollup 1:

Organizational Rollup 2:

Organizational Rollup 3:

Reporting Person

Last Name	First Name	M	Linked
McIntyre	Keith	R	

Responsible Supervisor

Last Name	First Name	M	Linked
Jordon	Minnie	K	

Building Name: North

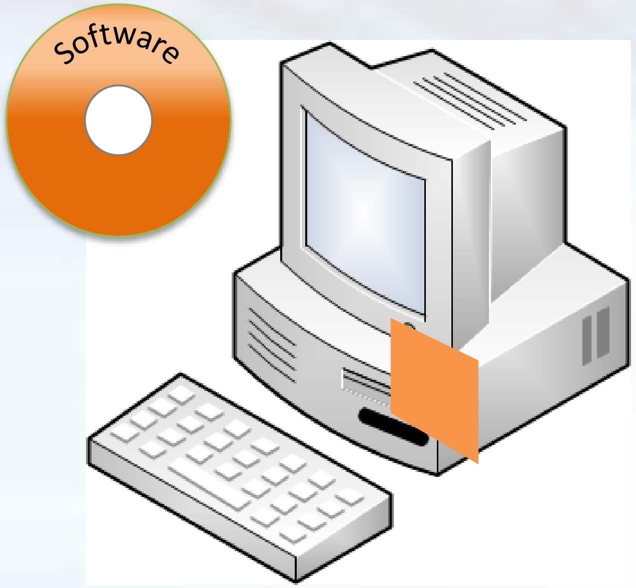
Location: Parking Lot

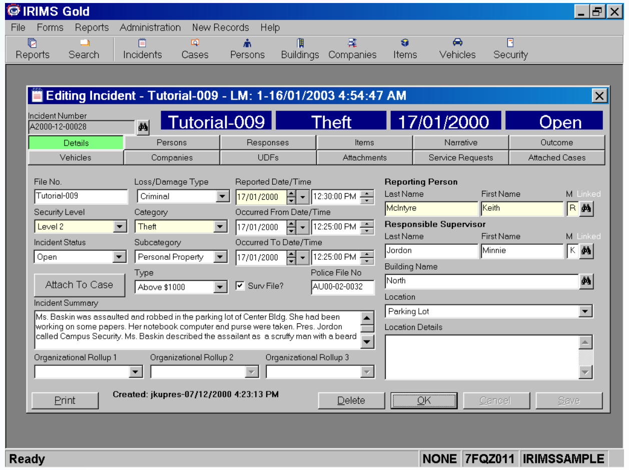
Location Details:

Created: jkupres-07/12/2000 4:23:13 PM

Ready | NONE | 7FQZ011 | IRIMSSAMPLE

COMPUTING THE OLD WAY





Editing Incident - Tutorial-009 - LM: 1-16/01/2003 4:54:47 AM

Incident Number: A2000-12-00028

Tutorial-009 | Theft | 17/01/2000 | Open

File No.: Tutorial-009
Loss/Damage Type: Criminal
Reported Date/Time: 17/01/2000 12:30:00 PM
Security Level: Level 2
Category: Theft
Occurred From Date/Time: 17/01/2000 12:25:00 PM
Incident Status: Open
Subcategory: Personal Property
Occurred To Date/Time: 17/01/2000 12:25:00 PM
Type: Above $1000
☑ Surv File?
Police File No: AU00-02-0032

Incident Summary:
Ms. Baskin was assaulted and robbed in the parking lot of Center Bldg. She had been working on some papers. Her notebook computer and purse were taken. Pres. Jordon called Campus Security. Ms. Baskin described the assailant as a scruffy man with a beard

Organizational Rollup 1:
Organizational Rollup 2:
Organizational Rollup 3:

Reporting Person
Last Name: McIntyre First Name: Keith M: R Linked

Responsible Supervisor
Last Name: Jordon First Name: Minnie M: K Linked

Building Name: North
Location: Parking Lot
Location Details:

Created: jkupres-07/12/2000 4:23:13 PM

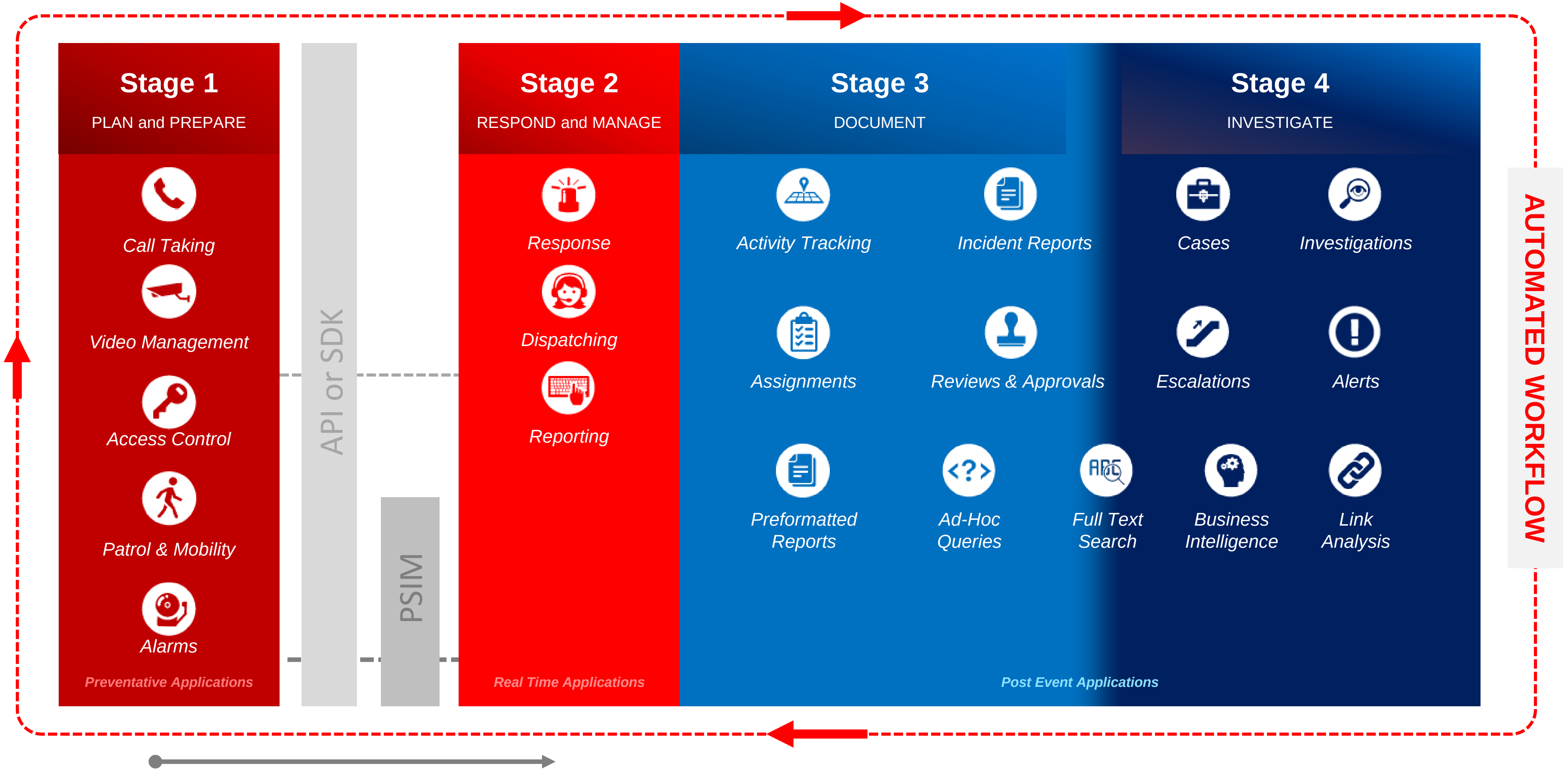
Ready | NONE | 7FQZ011 | IRIMSSAMPLE

COMPUTING THE NEW WAY

- API’s
- IP Based Programs
- Data & software in cloud
- Automatic sync

INTEGRATED INCIDENT MANAGEMENT

Interact. Communicate. Integrate.



Stage 1

PLAN and PREPARE

Call Taking

Video Management

Access Control

Patrol & Mobility

Alarms

Preventative Applications

API or SDK

PSIM

Stage 2

RESPOND and MANAGE

Response

Dispatching

Reporting

Real Time Applications

Stage 3

DOCUMENT

Activity Tracking

Incident Reports

Assignments

Reviews & Approvals

Preformatted Reports

Ad-Hoc Queries

Full Text Search

Stage 4

INVESTIGATE

Cases

Investigations

Escalations

Alerts

Business Intelligence

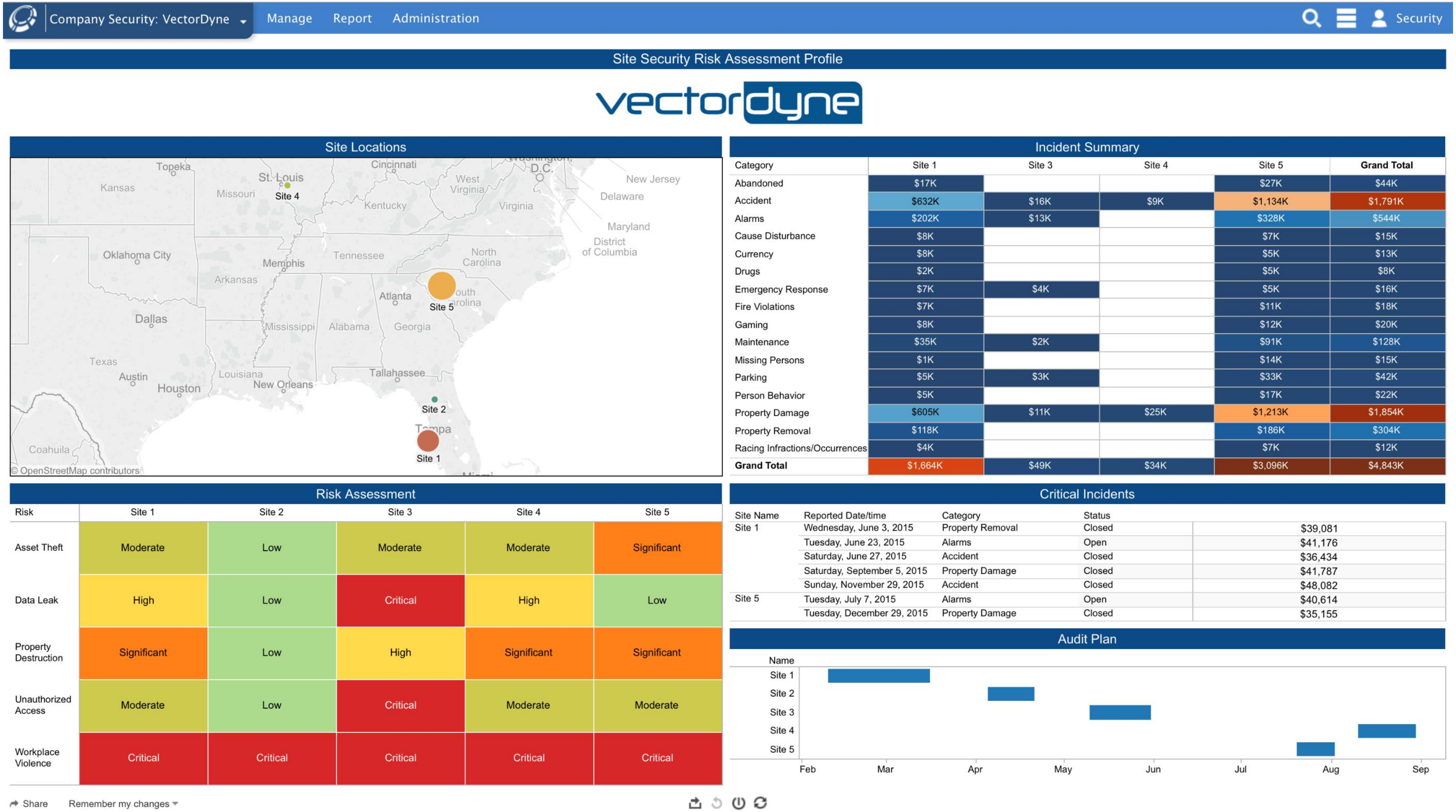
Link Analysis

Post Event Applications

AUTOMATED WORKFLOW

TYPICAL Security Management Process

COMPLETE Security Management Process



Site Security Risk Assessment Profile

vectordyne

Site Locations

Incident Summary

Category	Site 1	Site 3	Site 4	Site 5	Grand Total
Abandoned	$17K			$27K	$44K
Accident	$632K	$16K	$9K	$1,134K	$1,791K
Alarms	$202K	$13K		$328K	$544K
Cause Disturbance	$8K			$7K	$15K
Currency	$8K			$5K	$13K
Drugs	$2K			$5K	$8K
Emergency Response	$7K	$4K		$5K	$16K
Fire Violations	$7K			$11K	$18K
Gaming	$8K			$12K	$20K
Maintenance	$35K	$2K		$91K	$128K
Missing Persons	$1K			$14K	$15K
Parking	$5K	$3K		$33K	$42K
Person Behavior	$5K			$17K	$22K
Property Damage	$605K	$11K	$25K	$1,213K	$1,854K
Property Removal	$118K			$186K	$304K
Racing Infractions/Occurrences	$4K			$7K	$12K
Grand Total	$1,664K	$49K	$34K	$3,096K	$4,843K

Risk Assessment

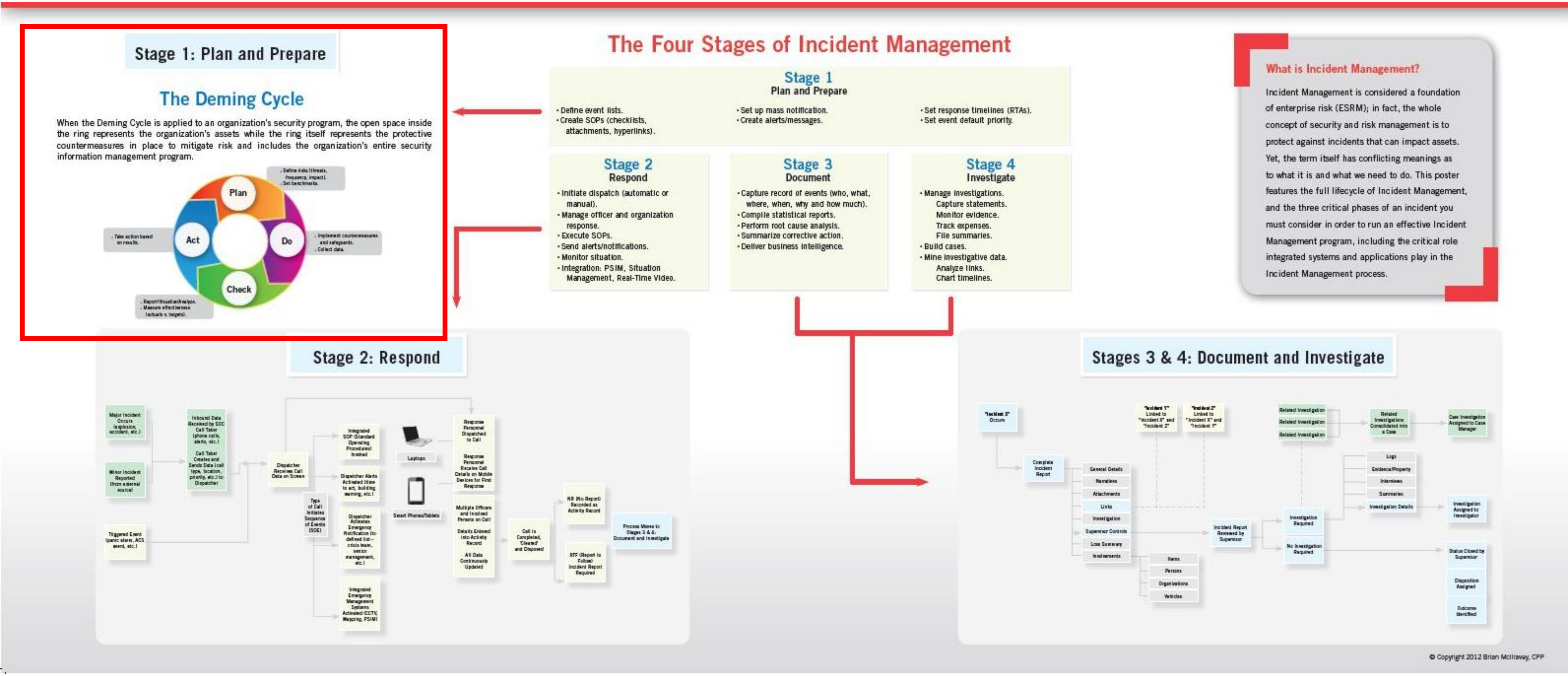
Risk	Site 1	Site 2	Site 3	Site 4	Site 5
Asset Theft	Moderate	Low	Moderate	Moderate	Significant
Data Leak	High	Low	Critical	High	Low
Property Destruction	Significant	Low	High	Significant	Significant
Unauthorized Access	Moderate	Low	Critical	Moderate	Moderate
Workplace Violence	Critical	Critical	Critical	Critical	Critical

Critical Incidents

Site Name	Reported Date/time	Category	Status	
Site 1	Wednesday, June 3, 2015	Property Removal	Closed	$39,081
	Tuesday, June 23, 2015	Alarms	Open	$41,176
	Saturday, June 27, 2015	Accident	Closed	$36,434
	Saturday, September 5, 2015	Property Damage	Closed	$41,787
	Sunday, November 29, 2015	Accident	Closed	$48,082
Site 5	Tuesday, July 7, 2015	Alarms	Open	$40,614
	Tuesday, December 29, 2015	Property Damage	Closed	$35,155

Audit Plan

Risk Process Relative to Incidents



Stage 1: Plan and Prepare

The Deming Cycle

When the Deming Cycle is applied to an organization's security program, the open space inside the ring represents the organization's assets while the ring itself represents the protective countermeasures in place to mitigate risk and includes the organization's entire security information management program.

Plan
- Define risks (threats, frequency, impact).
- Set benchmarks.
Do
- Implement countermeasures and safeguards.
- Collect data.
Check
- Report/Visualize/Analyze.
- Measure effectiveness (actuals v. targets).
Act
- Take action based on results.

The Four Stages of Incident Management

Stage 1
Plan and Prepare

- Define event lists.
- Create SOPs (checklists, attachments, hyperlinks).
- Set up mass notification.
- Create alerts/messages.
- Set response timelines (RTAs).
- Set event default priority.

Stage 2
Respond

- Initiate dispatch (automatic or manual).
- Manage officer and organization response.
- Execute SOPs.
- Send alerts/notifications.
- Monitor situation.
- Integration: PSIM, Situation Management, Real-Time Video.

Stage 3
Document

- Capture record of events (who, what, where, when, why and how much).
- Compile statistical reports.
- Perform root cause analysis.
- Summarize corrective action.
- Deliver business intelligence.

Stage 4
Investigate

- Manage investigations.
  Capture statements.
  Monitor evidence.
  Track expenses.
  File summaries.
- Build cases.
- Mine investigative data.
  Analyze links.
  Chart timelines.

What is Incident Management?

Incident Management is considered a foundation of enterprise risk (ESRM); in fact, the whole concept of security and risk management is to protect against incidents that can impact assets. Yet, the term itself has conflicting meanings as to what it is and what we need to do. This poster features the full lifecycle of Incident Management, and the three critical phases of an incident you must consider in order to run an effective Incident Management program, including the critical role integrated systems and applications play in the Incident Management process.

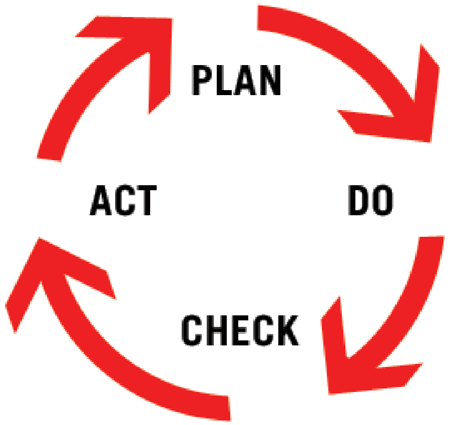
Stage 2: Respond

Major Incident Occurs (explosion, accident, etc.)
Minor Incident Reported (from external source)
Triggered Event (panic alarm, ACS event, etc.)
Inbound Data Received by SOC Call Taker (phone calls, alerts, etc.)
Call Taker Creates and Sends Data (call type, location, priority, etc.) to Dispatcher
Dispatcher Receives Call Data on Screen
Type of Call Initiates Sequence of Events (SOE)
Integrated SOP (Standard Operating Procedures) Invoked
Dispatcher Alerts Activated (time to act, building warning, etc.)
Dispatcher Activates Emergency Notification (to defined list – crisis team, senior management, etc.)
Integrated Emergency Management Systems Activated (CCTV, Mapping, PSIM)
Laptops
Smart Phones/Tablets
Response Personnel Dispatched to Call
Response Personnel Receive Call Details on Mobile Devices for First Response
Multiple Officers and Involved Persons on Call
Details Entered into Activity Record
All Data Continuously Updated
Call is Completed, 'Cleared' and Disposed
NR (No Report) Recorded as Activity Record
RTF (Report to Follow) Incident Report Required
Process Moves to Stages 3 & 4: Document and Investigate

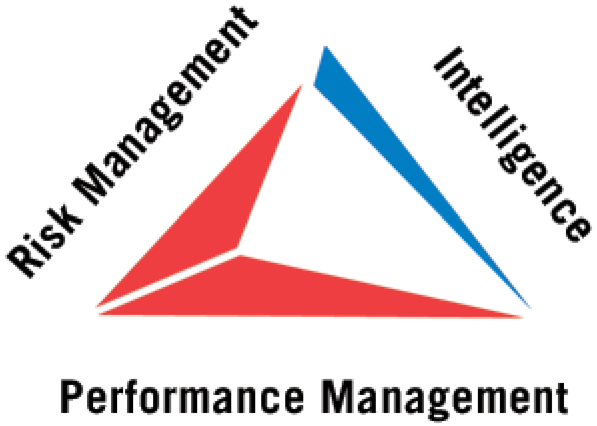
Stages 3 & 4: Document and Investigate

Angles of Incident Management

How does Incident Management fit into your risk management program?



The Deming Cycle



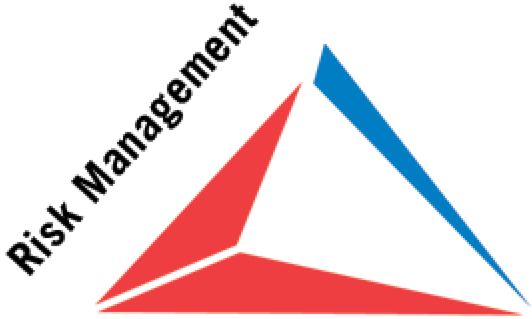
Angles of Incident Management

Risk Management

- Threat Frequency/Event History
- SLE
- ALE
- Freq Dist

Define Risks (Threats, Frequency, Impact)

INTERNAL THEFT



Take Action Based on Results

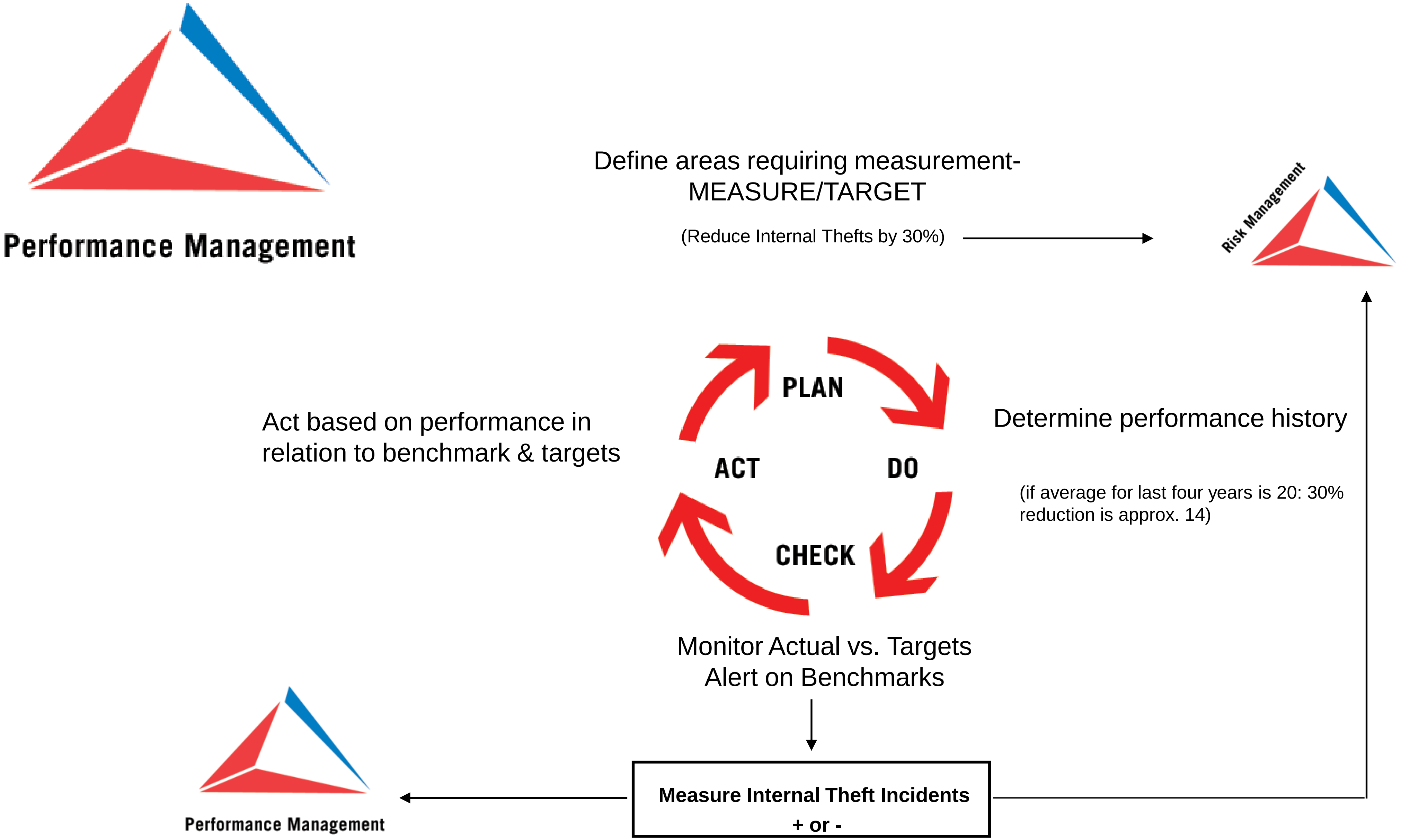
Implement Countermeasures
and Safeguards

Measure Effectiveness

↓

Incident Management
+ or -

Performance Measurement & Risk Management



Performance Management

Define areas requiring measurement-
MEASURE/TARGET

(Reduce Internal Thefts by 30%)

Risk Management

Act based on performance in relation to benchmark & targets

Determine performance history

(if average for last four years is 20: 30% reduction is approx. 14)

Monitor Actual vs. Targets
Alert on Benchmarks

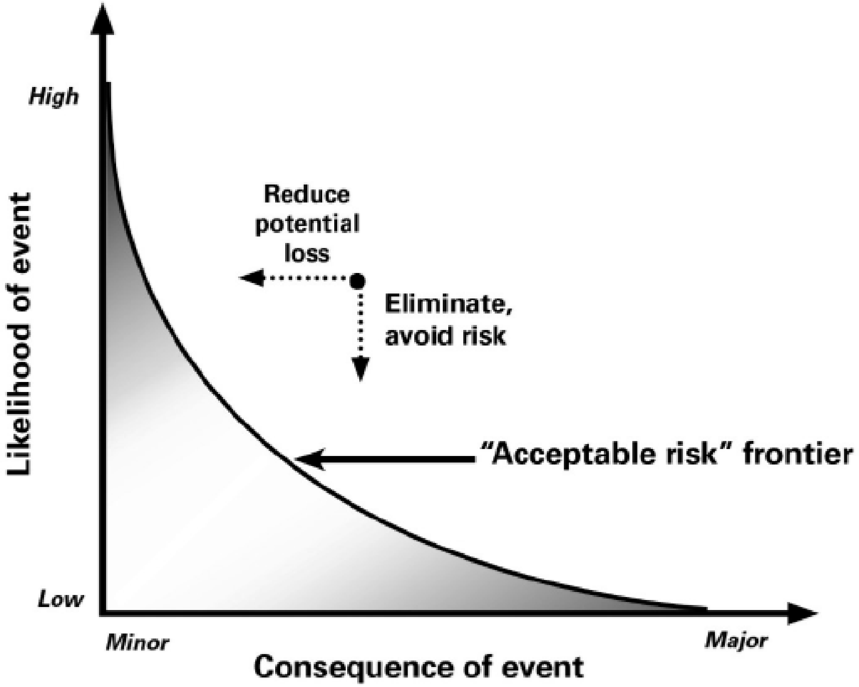
Measure Internal Theft Incidents
+ or -

Performance Management

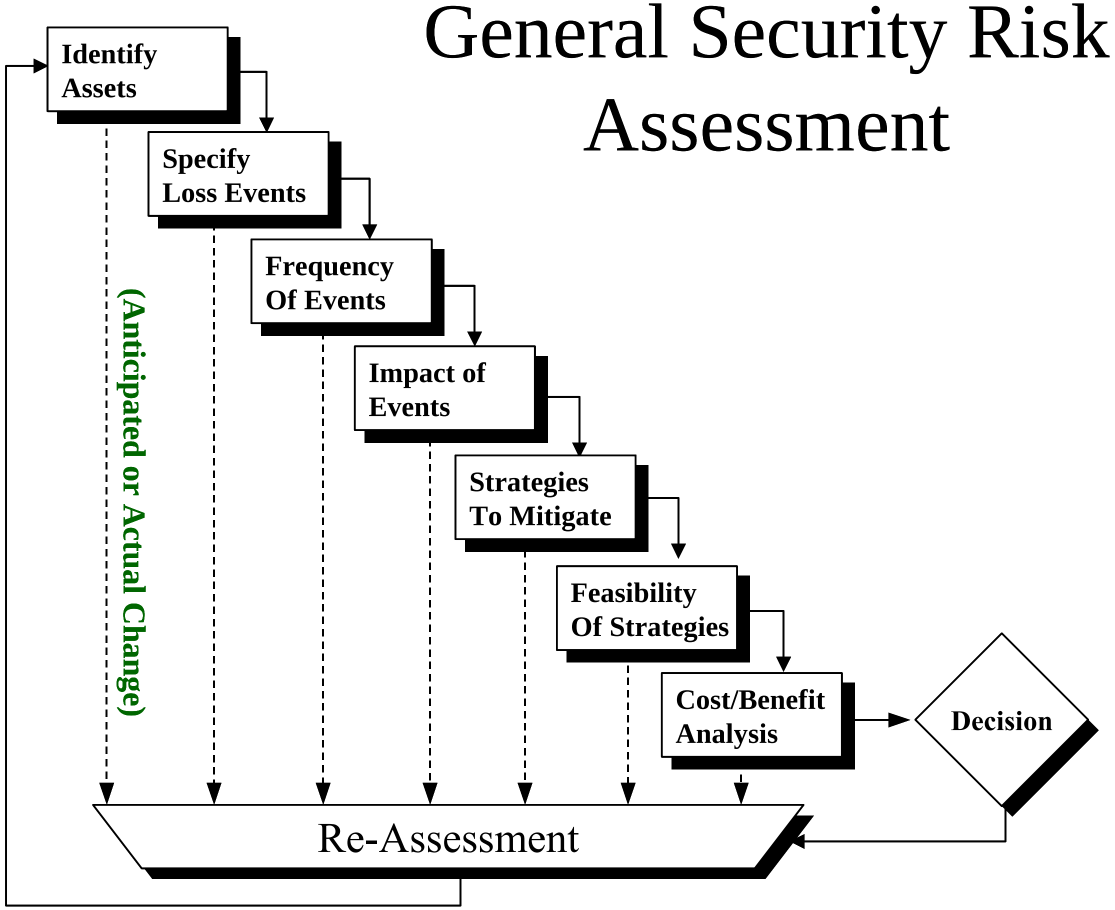
Risks = Threats x Vulnerabilities x Impact

Risks = Threats x Frequency x Impact

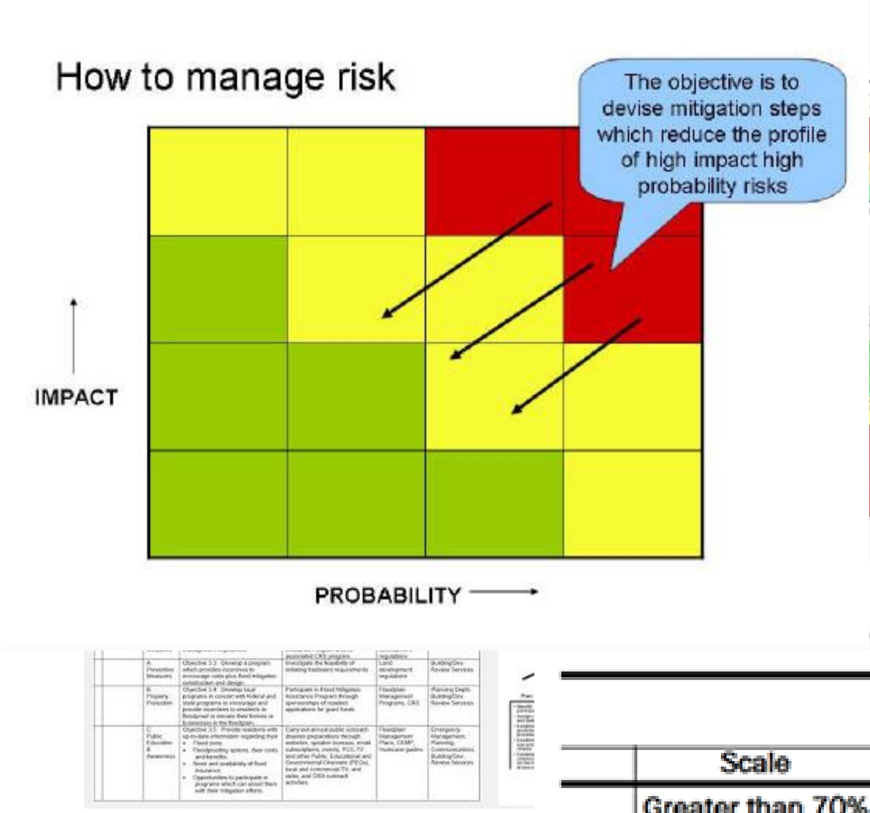
PA x (1-SE) x C$ = R$ + SE$

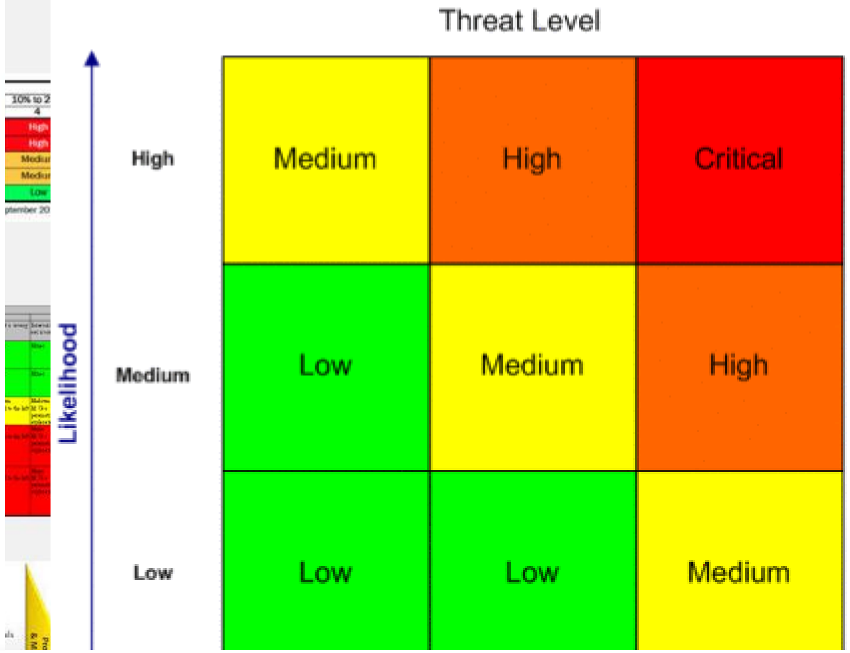


General Security Risk Assessment

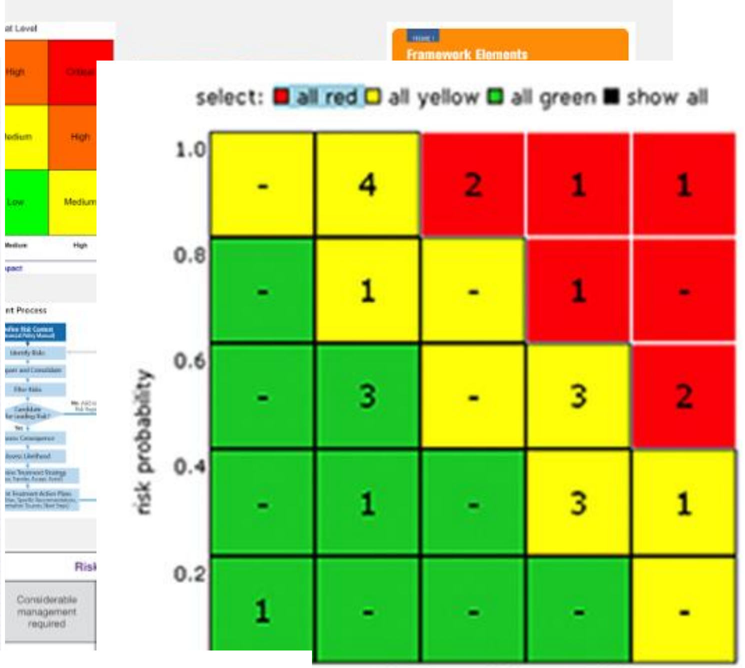


We Also See Risk by Color

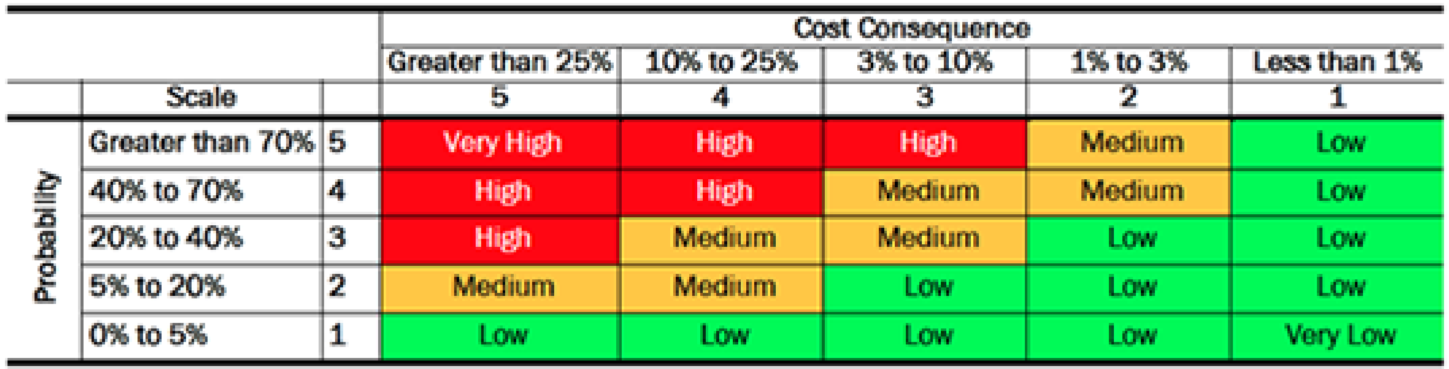

How to manage risk
The objective is to devise mitigation steps which reduce the profile of high impact high probability risks
IMPACT
PROBABILITY


Threat Level
Likelihood

Likelihood			
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Low	Low	Medium

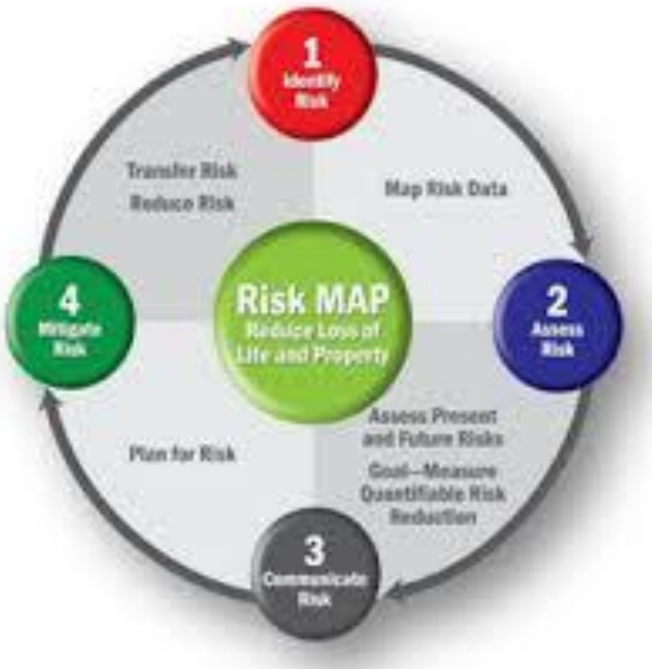


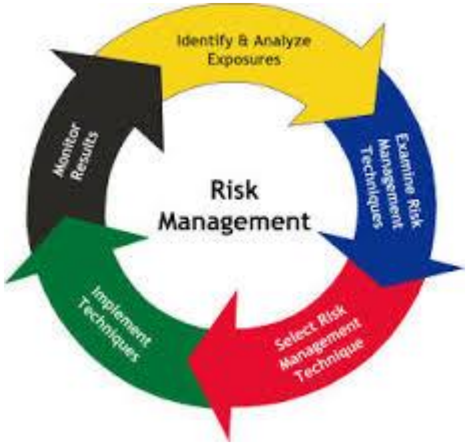
-	4	2	1	1
-	1	-	1	-
-	3	-	3	2
-	1	-	3	1
1	-	-	-	-

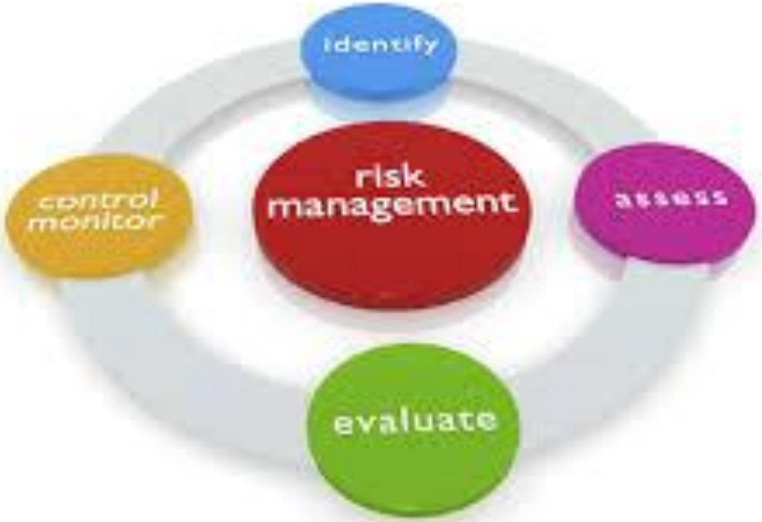


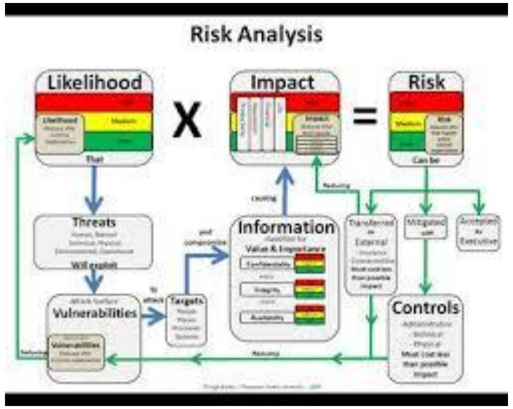
			Cost Consequence				
			Greater than 25%	10% to 25%	3% to 10%	1% to 3%	Less than 1%
	Scale		5	4	3	2	1
Probability	Greater than 70%	5	Very High	High	High	Medium	Low
	40% to 70%	4	High	High	Medium	Medium	Low
	20% to 40%	3	High	Medium	Medium	Low	Low
	5% to 20%	2	Medium	Medium	Low	Low	Low
	0% to 5%	1	Low	Low	Low	Low	Very Low

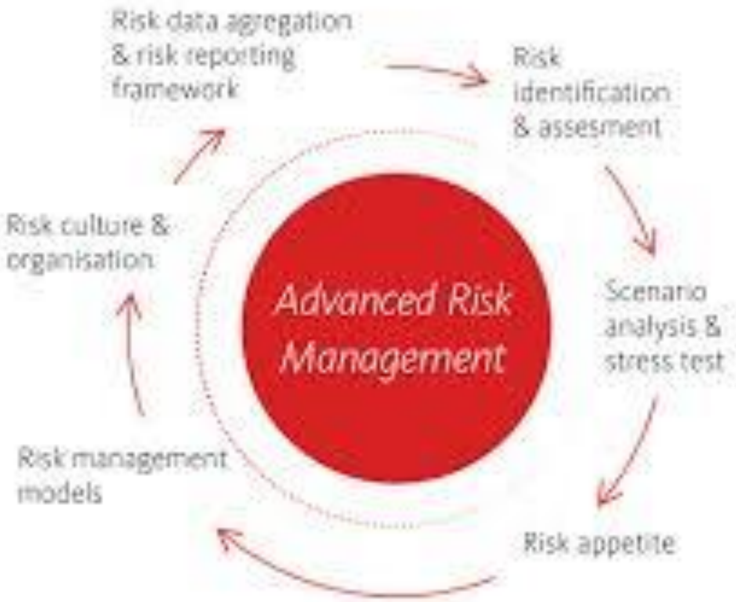
Source: Virginia DOT's PPTA Risk Analysis Guidance, September 2011

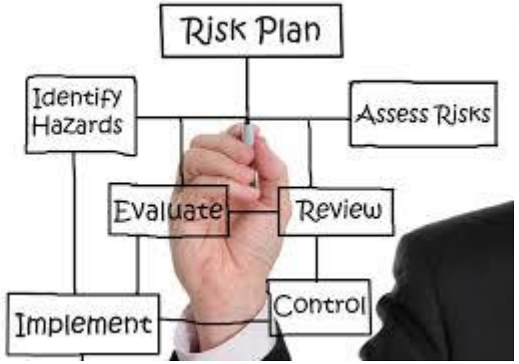

1
Identify
Risk
Map Risk Data
2
Assess
Risk
Assess Present
and Future Risks
Goal—Measure
Quantifiable Risk
Reduction
3
Communicate
Risk
Plan for Risk
4
Mitigate
Risk
Transfer Risk
Reduce Risk
Risk MAP
Reduce Loss of
Life and Property


Identify & Analyze
Exposures
Examine Risk
Management
Techniques
Select Risk
Management
Technique
Implement
Techniques
Monitor
Results
Risk
Management

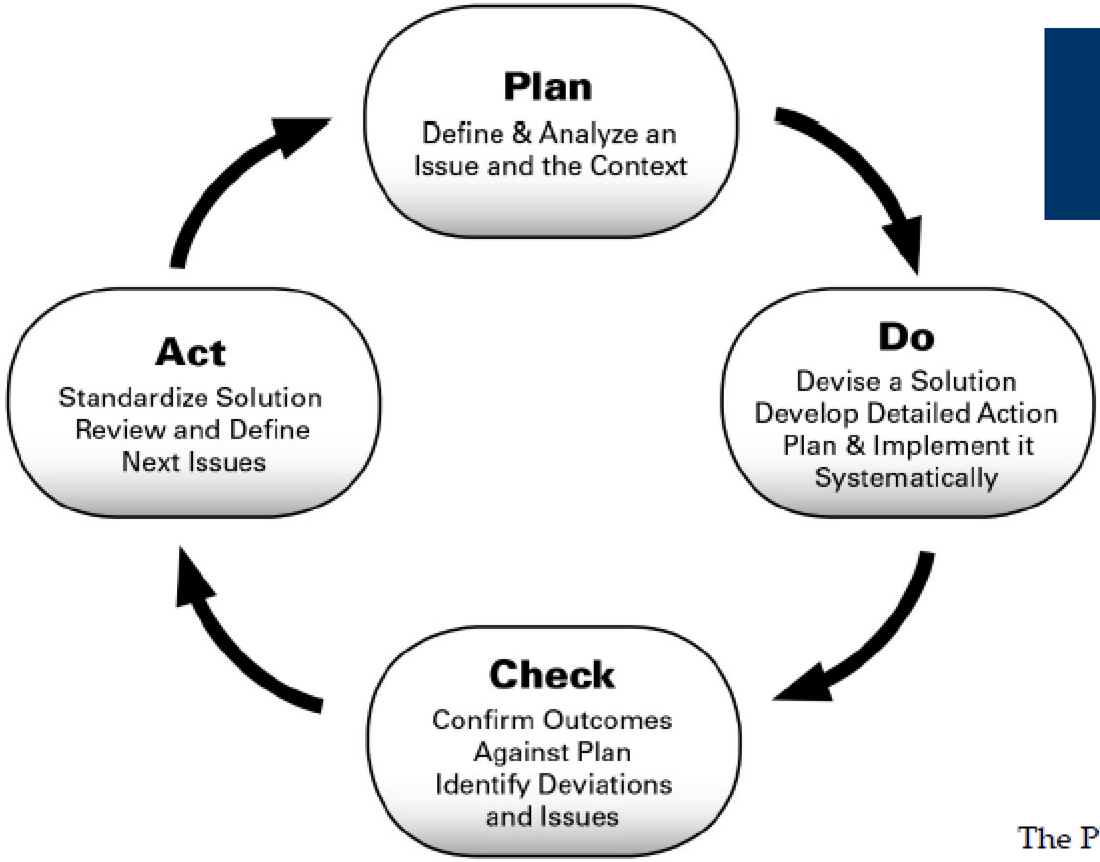

identify
assess
evaluate
control
monitor
risk
management


Risk Analysis
Likelihood
X
Impact
=
Risk
Medium
That
Can be
Threats
Will exploit
Vulnerabilities
Targets
Information
Value & Importance
Confidentiality
Integrity
Availability
causing
Reducing
Transferred
External
Must cost less
than possible
impact
Mitigated
Accepted
Executive
Controls
Must cost less
than possible
impact
Reducing


Risk data agregation
& risk reporting
framework
Risk
identification
& assesment
Scenario
analysis &
stress test
Risk appetite
Risk management
models
Risk culture &
organisation
Advanced Risk
Management


Risk Plan
Identify
Hazards
Assess Risks
Evaluate
Review
Implement
Control

2015-2016 ASIS ANSI Risk Assessment Model


Plan
Define & Analyze an Issue and the Context
Do
Devise a Solution Develop Detailed Action Plan & Implement it Systematically
Check
Confirm Outcomes Against Plan Identify Deviations and Issues
Act
Standardize Solution Review and Define Next Issues

The PDCA model is a clear, systematic, and documented approach to:

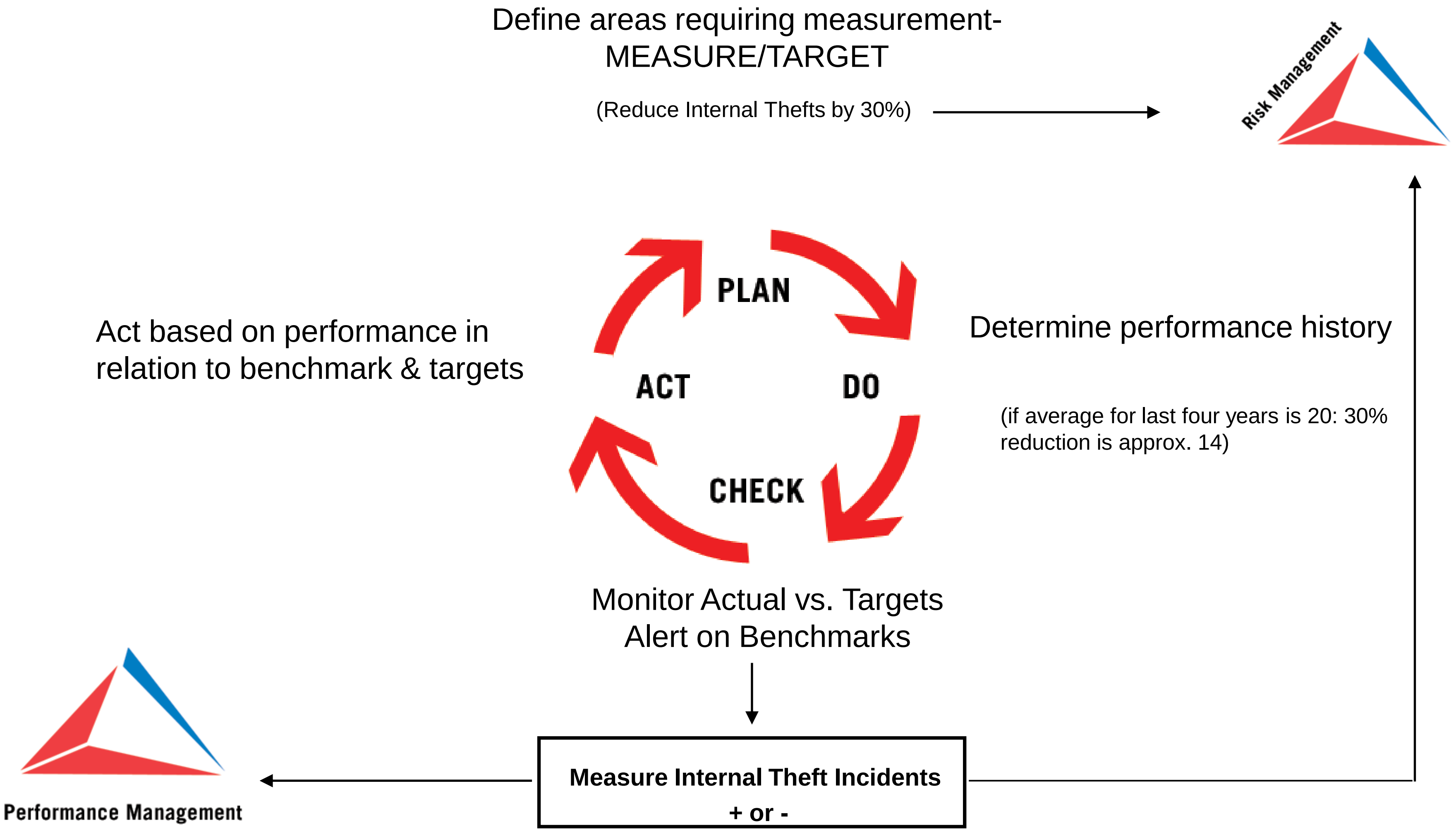
a) Set measurable policies, objectives, and targets;

b) Methodically implement the program;

c) Monitor, measure, and evaluate progress;

d) Identify, prevent, or remedy problems as they occur;

Performance Measurement & Risk Management



Define areas requiring measurement-
MEASURE/TARGET

(Reduce Internal Thefts by 30%)

Determine performance history

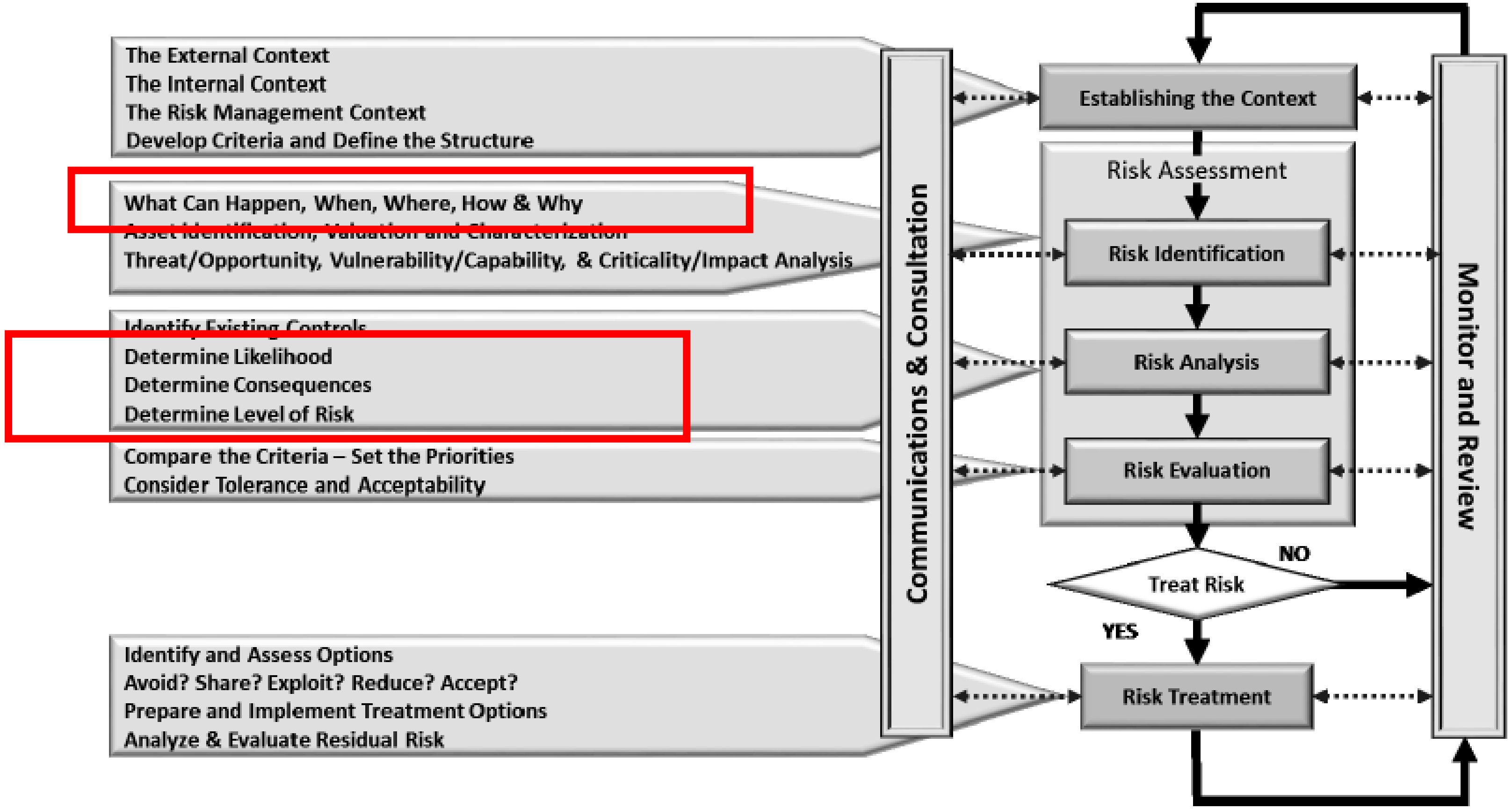
(if average for last four years is 20: 30%
reduction is approx. 14)

Monitor Actual vs. Targets
Alert on Benchmarks

Measure Internal Theft Incidents
+ or -

Act based on performance in
relation to benchmark & targets

ANSI/ASIS/RIMS RA.1-2015



The External Context
The Internal Context
The Risk Management Context
Develop Criteria and Define the Structure

What Can Happen, When, Where, How & Why
Asset Identification, Valuation and Characterization
Threat/Opportunity, Vulnerability/Capability, & Criticality/Impact Analysis

Identify Existing Controls
Determine Likelihood
Determine Consequences
Determine Level of Risk

Compare the Criteria – Set the Priorities
Consider Tolerance and Acceptability

Identify and Assess Options
Avoid? Share? Exploit? Reduce? Accept?
Prepare and Implement Treatment Options
Analyze & Evaluate Residual Risk

Communications & Consultation

Establishing the Context

Risk Assessment

Risk Identification

Risk Analysis

Risk Evaluation

Treat Risk

NO

YES

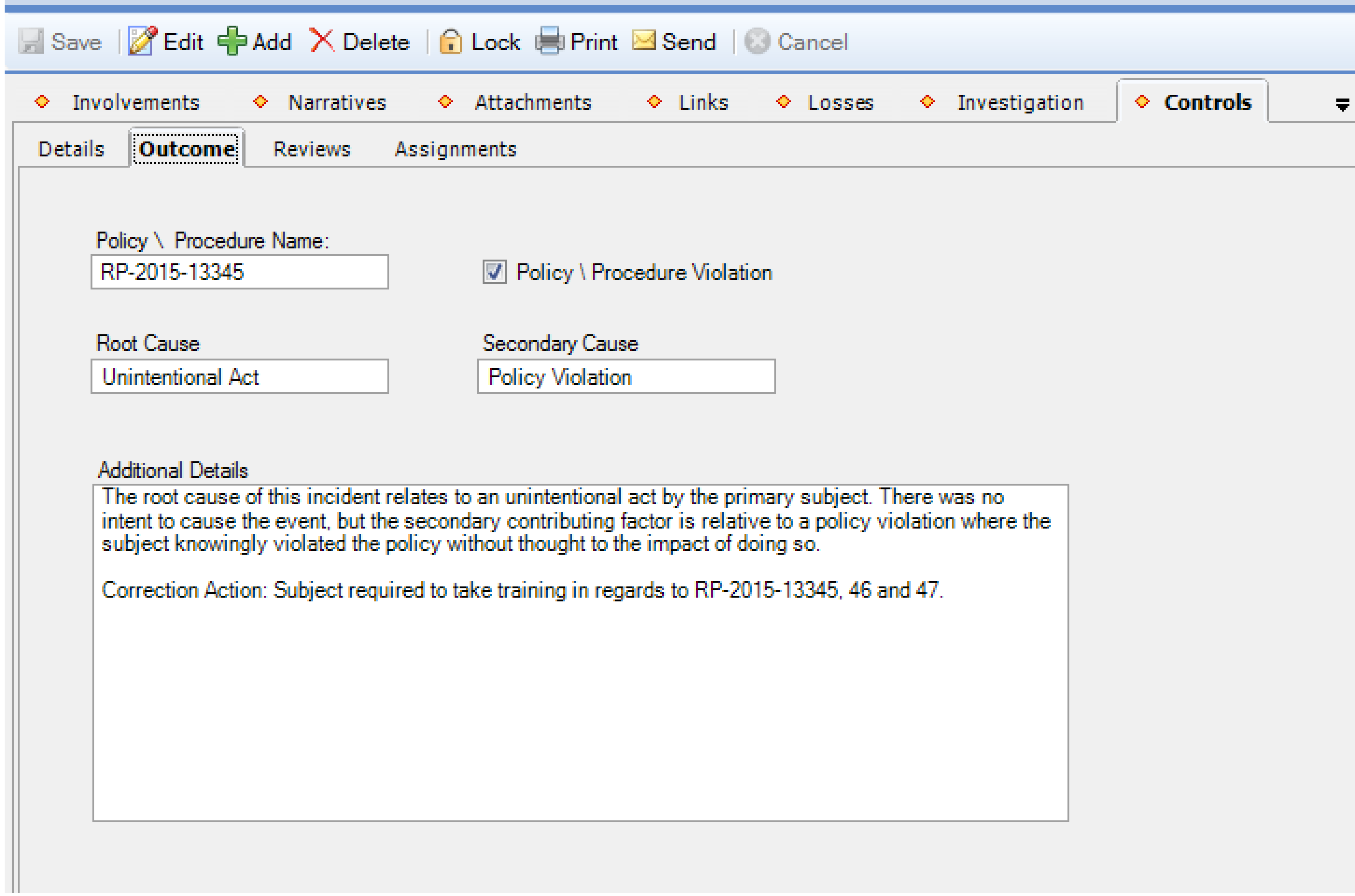
Risk Treatment

Monitor and Review

Figure 1: Risk Management Process (based on ISO 31000)

How and Why

Cause
Mechanism
Manner



Policy \ Procedure Name: RP-2015-13345

☑ Policy \ Procedure Violation

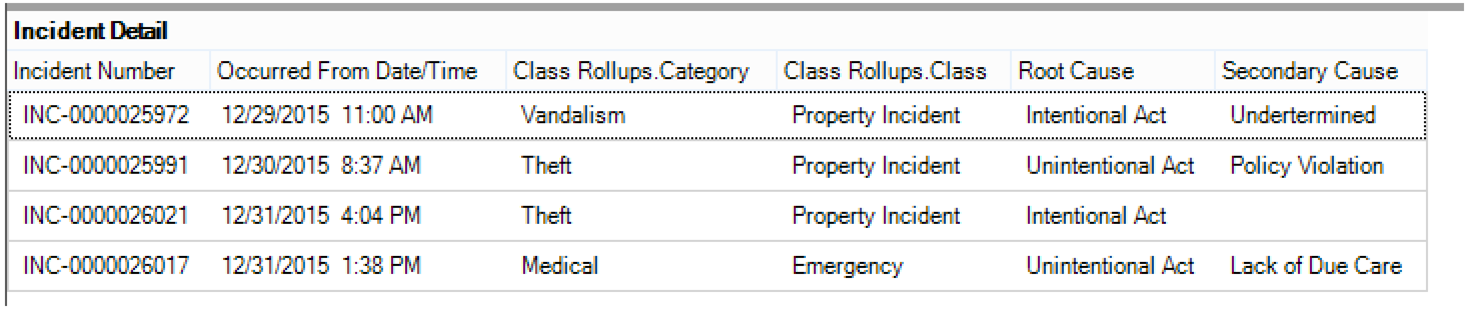
Root Cause: Unintentional Act

Secondary Cause: Policy Violation

Additional Details

The root cause of this incident relates to an unintentional act by the primary subject. There was no intent to cause the event, but the secondary contributing factor is relative to a policy violation where the subject knowingly violated the policy without thought to the impact of doing so.

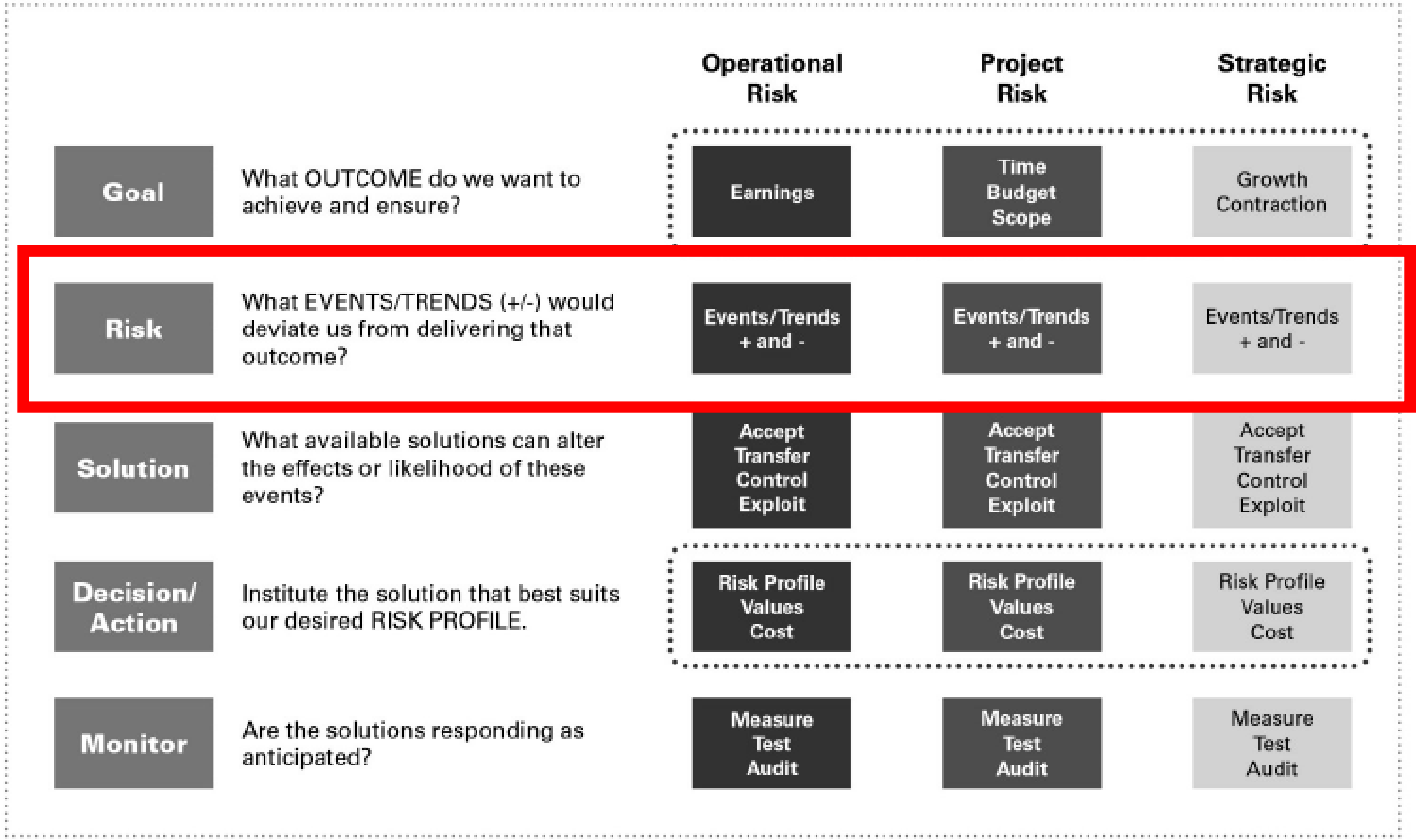
Correction Action: Subject required to take training in regards to RP-2015-13345, 46 and 47.



Incident Detail

Incident Number	Occurred From Date/Time	Class Rollups.Category	Class Rollups.Class	Root Cause	Secondary Cause
INC-0000025972	12/29/2015 11:00 AM	Vandalism	Property Incident	Intentional Act	Undertermined
INC-0000025991	12/30/2015 8:37 AM	Theft	Property Incident	Unintentional Act	Policy Violation
INC-0000026021	12/31/2015 4:04 PM	Theft	Property Incident	Intentional Act	
INC-0000026017	12/31/2015 1:38 PM	Medical	Emergency	Unintentional Act	Lack of Due Care

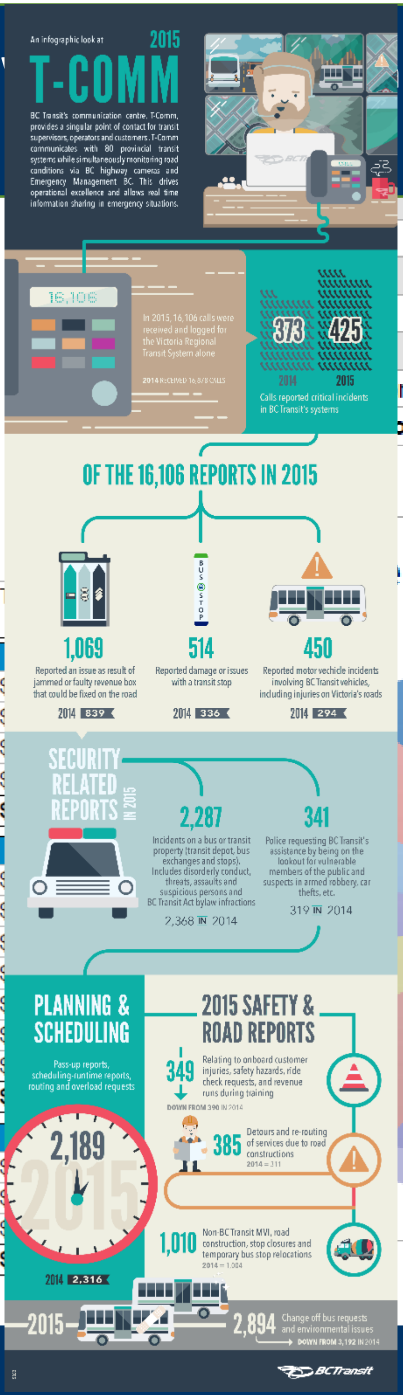
ANSI/ASIS/RIMS RA.1-2015



		Operational Risk	Project Risk	Strategic Risk
Goal	What OUTCOME do we want to achieve and ensure?	Earnings	Time Budget Scope	Growth Contraction
Risk	What EVENTS/TRENDS (+/-) would deviate us from delivering that outcome?	Events/Trends + and -	Events/Trends + and -	Events/Trends + and -
Solution	What available solutions can alter the effects or likelihood of these events?	Accept Transfer Control Exploit	Accept Transfer Control Exploit	Accept Transfer Control Exploit
Decision/ Action	Institute the solution that best suits our desired RISK PROFILE.	Risk Profile Values Cost	Risk Profile Values Cost	Risk Profile Values Cost
Monitor	Are the solutions responding as anticipated?	Measure Test Audit	Measure Test Audit	Measure Test Audit

Dangerous Condition	516	658	1174	621	804	1425	0	0	2599
Disaster	557	722	1279	674	908	1582	0	0	2861
Emergency Response	1081	1369	2450	1261	1653	2914	0	0	5364
General Assistance	222	281	503	272	366	638	0	0	1141
Property	77	127	204	115	139	254	0	0	458
Security Request	1003	1237	2240	1188	1513	2701	5	5	4946
Security Response	0	6	6	0	1	1	3	3	10
Total	3456	4400	7856	4131	5384	9515	8	8	17379

Category	Number of Incidents	Total Losses	Total Recoveries	Net Losses
Compliance \ Assessment				
Security	54	$0.00	$0.00	$0.00
Safety	53	$0.00	$0.00	$0.00
Fire	56	$0.00	$0.00	$0.00
	6	$2,904.00	$1,000.00	$1,904.00
Compliance \ Assessment Totals:	**169**	**$2,904.00**	**$1,000.00**	**$1,904.00**
Emergency				
Threats	528	$0.00	$0.00	$0.00
Natural Disaster	20	$0.00	$0.00	$0.00
Missing Person	201	$0.00	$0.00	$0.00
Medical	412	$1,000.00	$0.00	$1,000.00
Fire Response	209	$0.00	$0.00	$0.00
Building	654	$10,456.00	$4,560.00	$5,896.00
	3	$0.00	$0.00	$0.00
Emergency Totals:	**2,027**	**$11,456.00**	**$4,560.00**	**$6,896.00**
Human Resources				
Investigation	324	$0.00	$0.00	$0.00
Employee Misconduct	163	$0.00	$0.00	$0.00
Assistance	279	$5,815.00	$500.00	$5,315.00
Human Resources Totals:	**766**	**$5,815.00**	**$500.00**	**$5,315.00**


An infographic look at

2015

T-COMM

BC Transit's communication centre, T-Comm, provides a singular point of contact for transit supervisors, operators and customers. T-Comm communicates with 80 provincial transit systems while simultaneously monitoring road conditions via BC highway cameras and Emergency Management BC. This drives operational excellence and allows real time information sharing in emergency situations.

16,106

In 2015, 16,106 calls were received and logged for the Victoria Regional Transit System alone

2014 RECEIVED 16,878 CALLS

373 2014 | 425 2015

Calls reported critical incidents in BC Transit's systems

OF THE 16,106 REPORTS IN 2015

1,069 Reported an issue as result of jammed or faulty revenue box that could be fixed on the road 2014 839

514 Reported damage or issues with a transit stop 2014 336

450 Reported motor vechicle incidents involving BC Transit vehicles, including injuries on Victoria's roads 2014 294

SECURITY RELATED REPORTS IN 2015

2,287 Incidents on a bus or transit property (transit depot, bus exchanges and stops). Includes disorderly conduct, threats, assaults and suspicious persons and BC Transit Act bylaw infractions 2,368 IN 2014

341 Police requesting BC Transit's assistance by being on the lookout for vulnerable members of the public and suspects in armed robbery, car thefts, etc. 319 IN 2014

PLANNING & SCHEDULING

Pass-up reports, scheduling-runtime reports, routing and overload requests

2,189 2015

2014 2,316

2015 SAFETY & ROAD REPORTS

349 Relating to onboard customer injuries, safety hazards, ride check requests, and revenue runs during training DOWN FROM 390 IN 2014

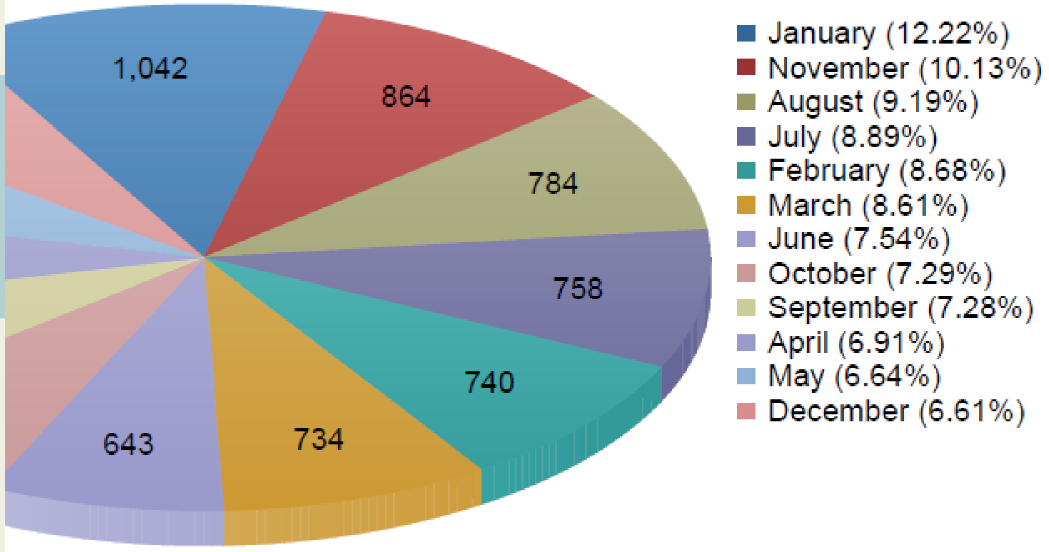
385 Detours and re-routing of services due to road constructions 2014 = 311

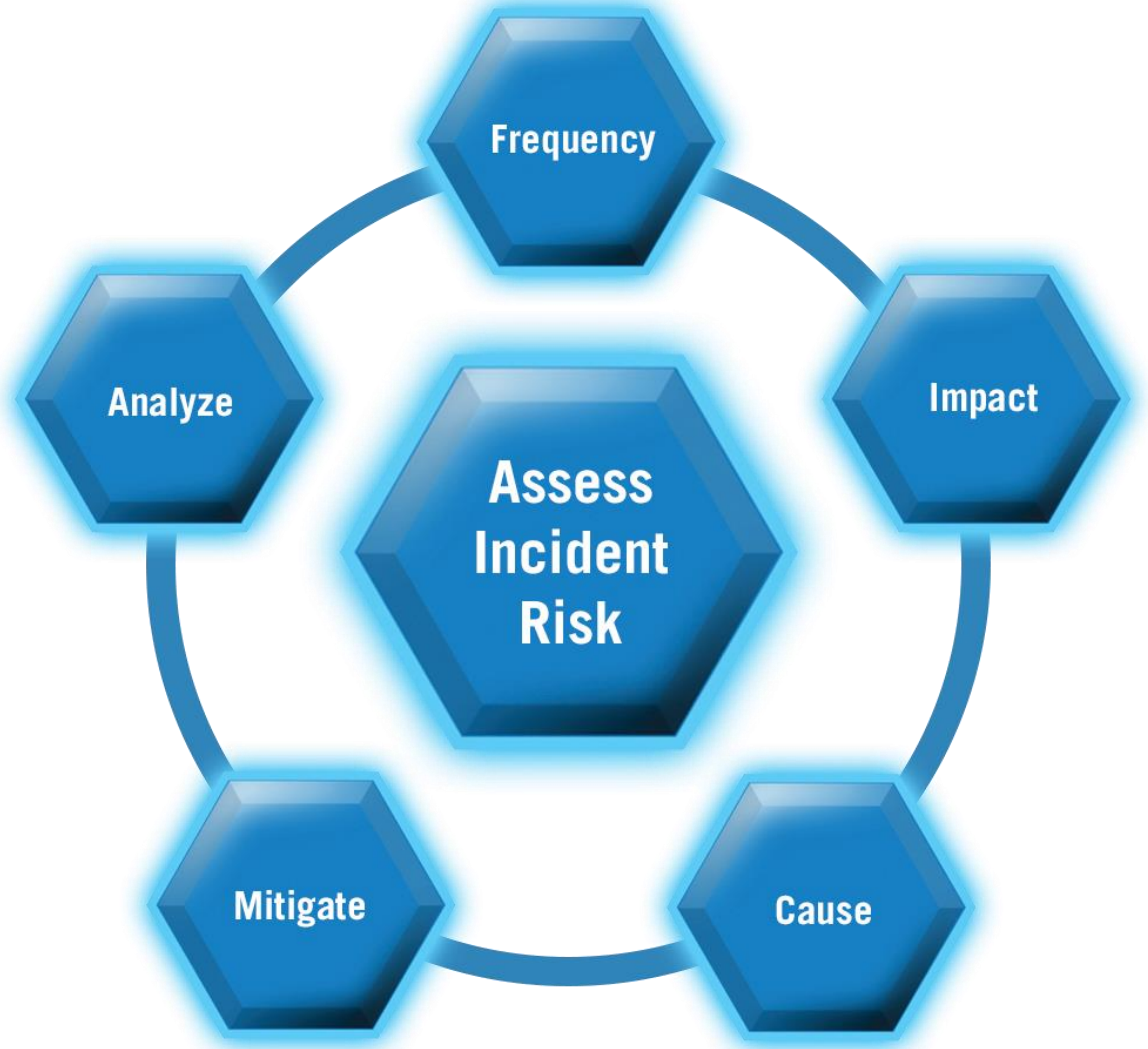
1,010 Non-BC Transit MVI, road construction, stop closures and temporary bus stop relocations 2014 = 1,004

2015 **2,894** Change off bus requests and environmental issues DOWN FROM 3,192 IN 2014

	128	97	83	66	80	85	96	102	84	103	122	73	1119
	85	59	66	44	37	51	86	37	64	33	60	47	**669**
	126	94	98	81	86	74	82	95	92	69	100	85	**1082**
	106	85	85	77	56	62	60	96	54	51	75	49	**856**
	113	81	84	56	66	68	125	82	66	81	106	59	**987**
n	4	4	6	2	2	4	5	9	0	4	8	10	**58**
otal	**1042**	**740**	**734**	**589**	**566**	**643**	**758**	**784**	**621**	**622**	**864**	**564**	**8527**

nt Breakdown by Month




Frequency
Analyze
Impact
Assess Incident Risk
Mitigate
Cause

ERM v. ESRM

Does the fact that security incidents represent a risk to the enterprise mean we are doing enterprise risk management?

“ESRM uses risk-management principles to manage security related risks across an enterprise. ESRM does not define an organizational structure. Enterprise Risk Management (ERM) uses risk-management principles to address enterprise risk issues and often defines an organisational structure. The security department may be represented within an ERM program if one exists, but ESRM is simply the processes under which the security department manages security-related risks.”

ESRM highlights the protection of assets and activities such as physical security, investigations, crisis management, business continuity, and data protection;

Security professionals are recognizing that whatever risks their organizations face, they need to reach across all business units to ensure that every department collaborates with the goals of enhancing security, increasing the bottom line, and assisting the organization in meeting its objectives. This is Enterprise Security Risk Management (ESRM). It is a vital element of Enterprise Risk Management (ERM), which examines the universe of risks—financial, strategic, operational, legal, accidental, and so on—that an organization faces.

IT HR Risk Management Legal Security Ethics Compliance Safety Environment

Incidents and Events at Departmental Level

ESRM Principles

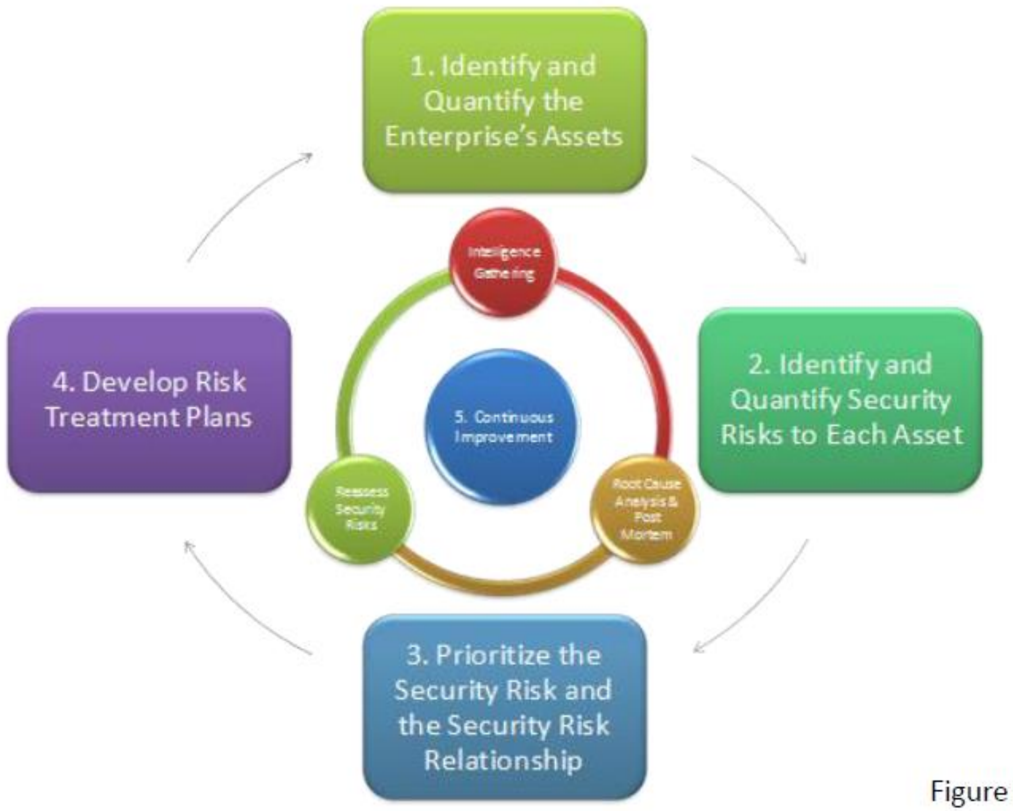
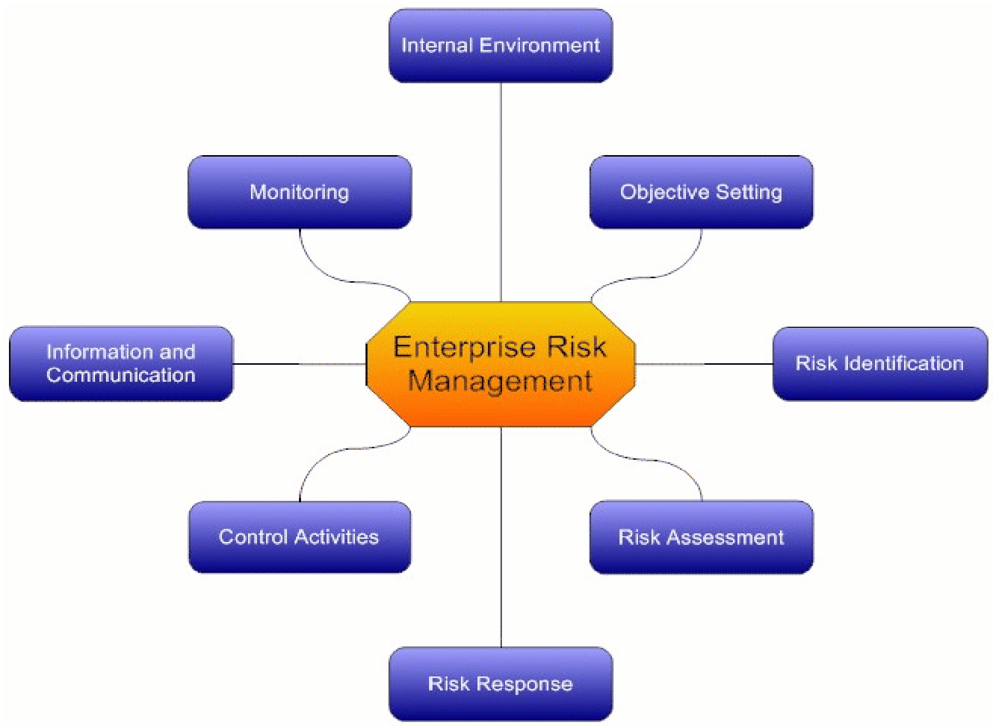
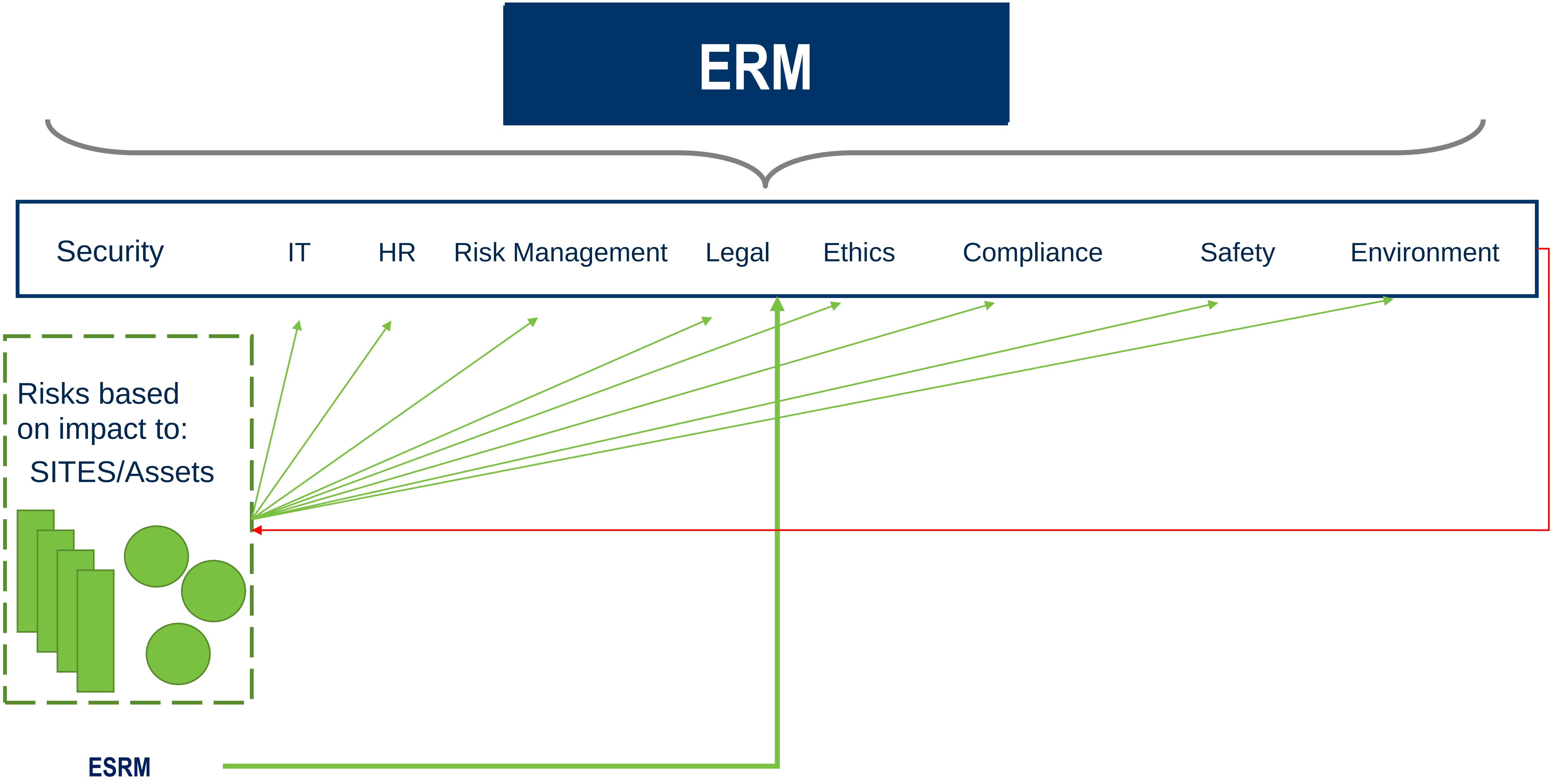

1. Identify and Quantify the Enterprise's Assets
2. Identify and Quantify Security Risks to Each Asset
3. Prioritize the Security Risk and the Security Risk Relationship
4. Develop Risk Treatment Plans
Intelligence Gathering
5. Continuous Improvement
Reassess Security Risks
Root Cause Analysis & Post Mortem

Figure 1



ERM*



ERM

Security IT HR Risk Management Legal Ethics Compliance Safety Environment

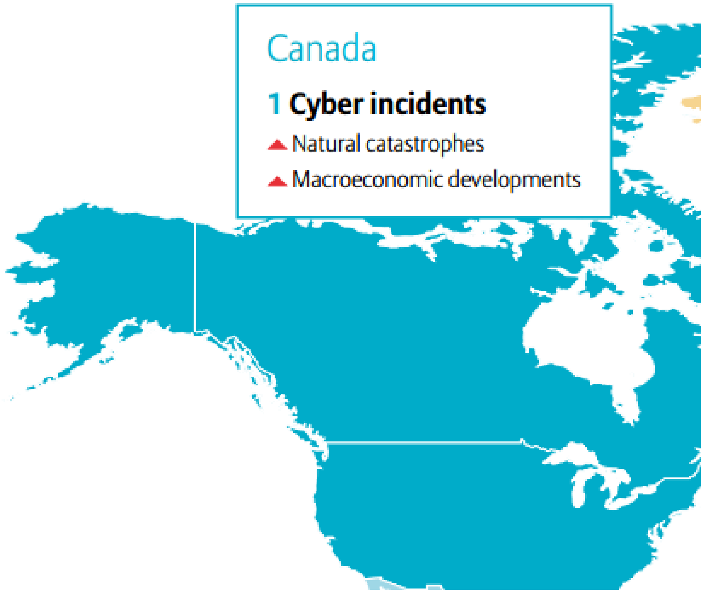
Risks based on impact to:

SITES/Assets

ESRM

SURVEY SAYS!!!

ALLIANZ RISK BAROMETER 2016



Canada

1 Cyber incidents

▲ Natural catastrophes

▲ Macroeconomic developments

Top 10 Global Business Risks for 2016

1 Business interruption (incl. supply chain disruption) 38% ◀▶ 2015: 1 (46%)

2 Market developments (volatility, intensified competition, market stagnation) 34% ▲ NEW

3 Cyber incidents (cyber crime, data breaches, IT failures) 28% ▲ 2015: 5 (17%)

4 Natural catastrophes (storm, flood, earthquake) 24% ▼ 2015: 2 (30%)

5 Changes in legislation and regulation (economic sanctions, protectionism) 24% ▼ 2015: 4 (18%)

6 Macroeconomic developments (austerity programs, commodity price increase, inflation/deflation) 22% ▲ NEW

7 Loss of reputation or brand value 18% ▼ 2015: 6 (16%)

8 Fire, explosion 16% ▼ 2015: 3 (27%)

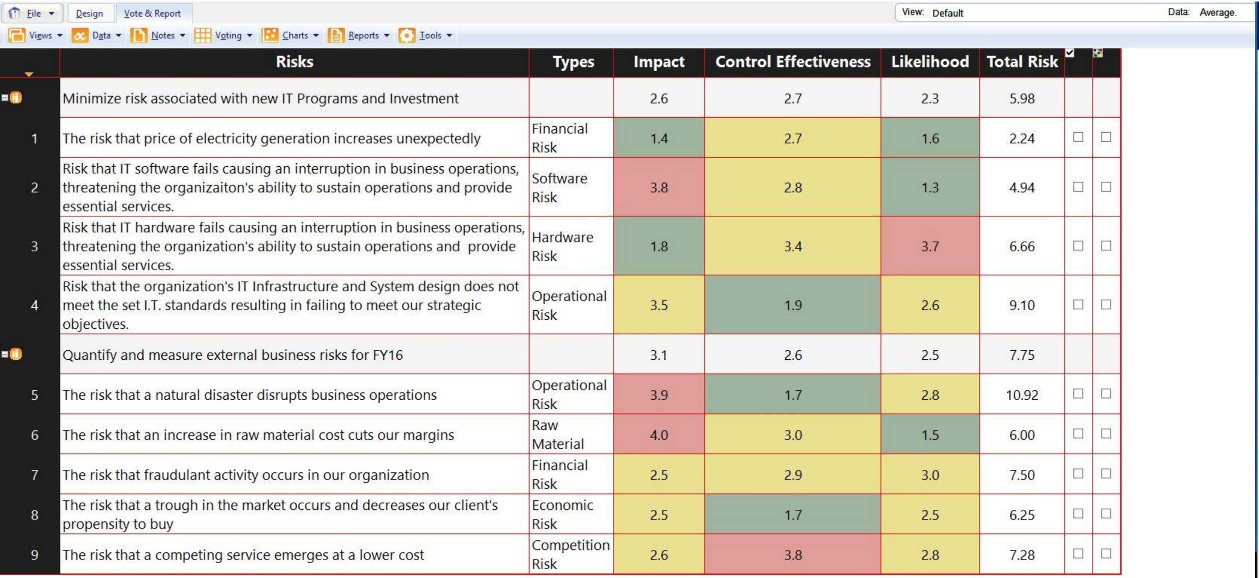
9 Political risks (war, terrorism, upheaval) 11% ◀▶ 2015: 9 (11%)

10 Theft, fraud and corruption 11% ◀▶ 2015: 10 (9%)

Which major causes of business interruption do businesses fear most?

Which trends will increase the threat of business interruption in future?

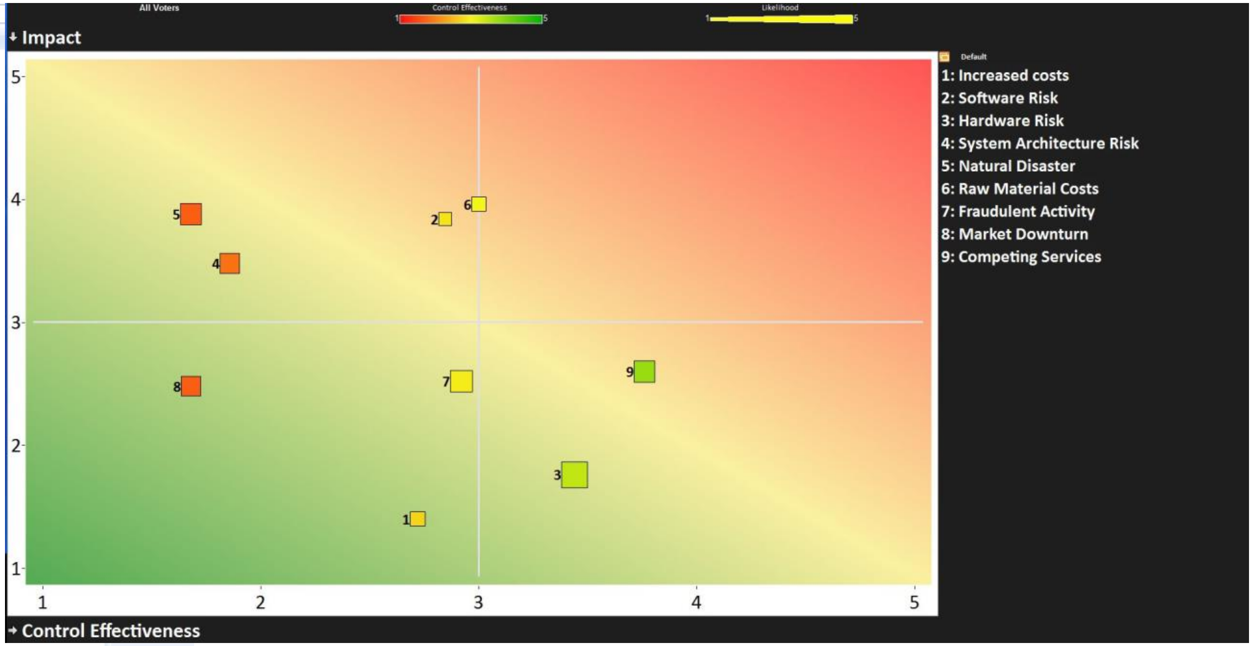
What’s this Ballot Survey Thing!!!

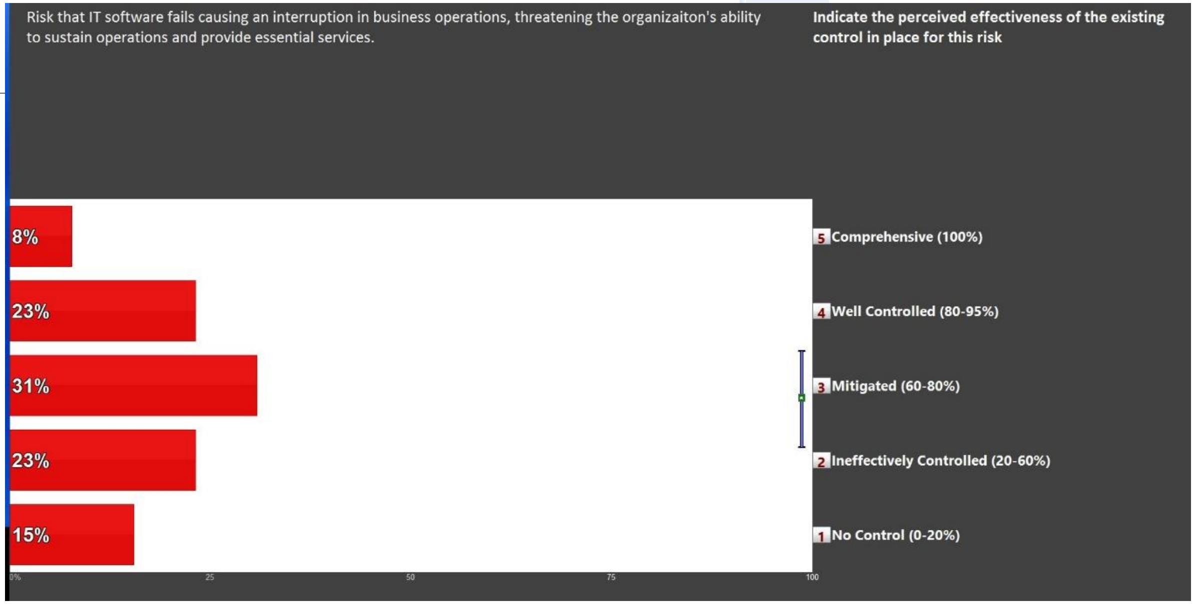


View: Default

Data: Average.

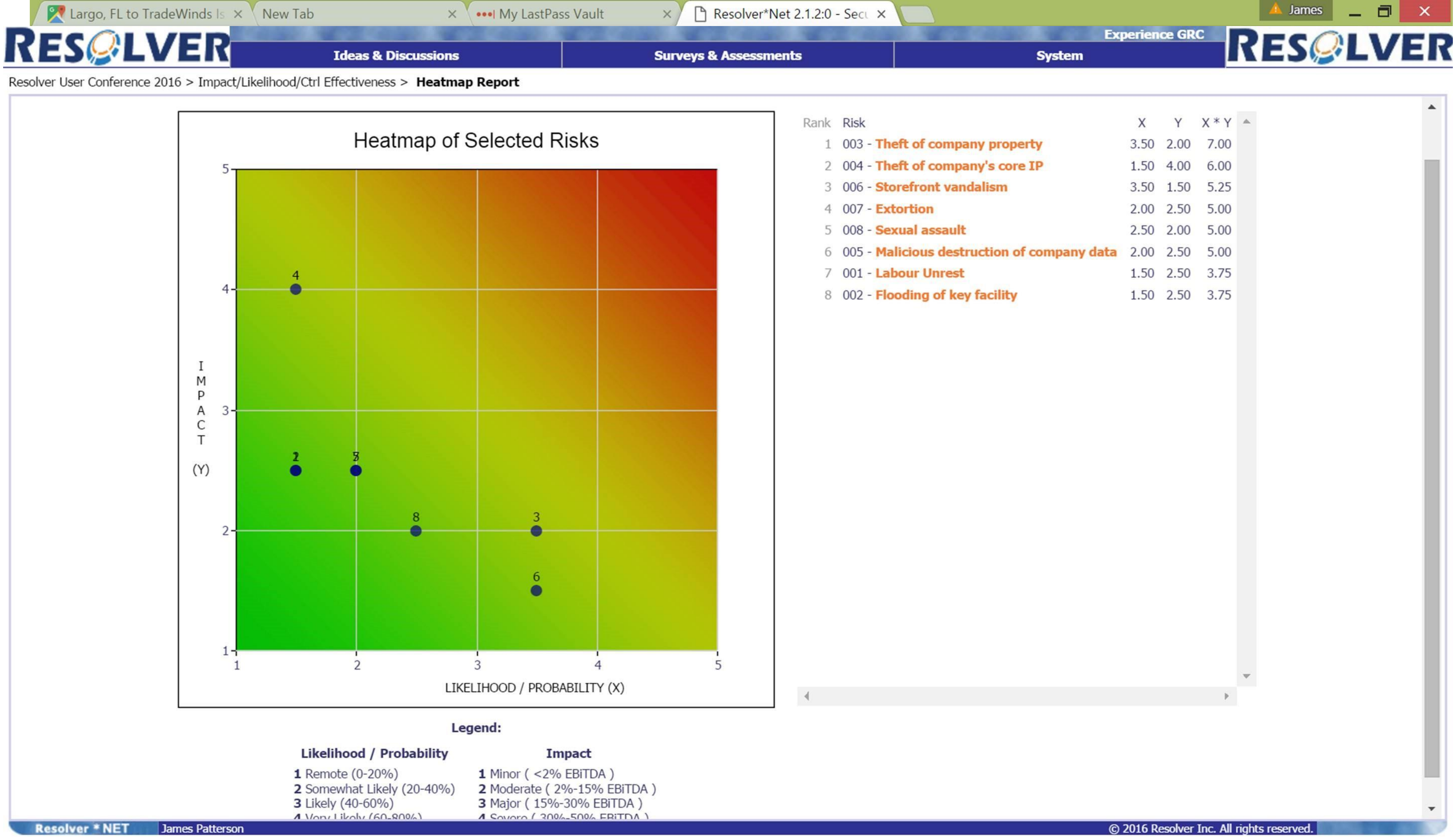
	Risks	Types	Impact	Control Effectiveness	Likelihood	Total Risk	☑	
	Minimize risk associated with new IT Programs and Investment		2.6	2.7	2.3	5.98		
1	The risk that price of electricity generation increases unexpectedly	Financial Risk	1.4	2.7	1.6	2.24	□	□
2	Risk that IT software fails causing an interruption in business operations, threatening the organizaiton's ability to sustain operations and provide essential services.	Software Risk	3.8	2.8	1.3	4.94	□	□
3	Risk that IT hardware fails causing an interruption in business operations, threatening the organization's ability to sustain operations and provide essential services.	Hardware Risk	1.8	3.4	3.7	6.66	□	□
4	Risk that the organization's IT Infrastructure and System design does not meet the set I.T. standards resulting in failing to meet our strategic objectives.	Operational Risk	3.5	1.9	2.6	9.10	□	□
	Quantify and measure external business risks for FY16		3.1	2.6	2.5	7.75		
5	The risk that a natural disaster disrupts business operations	Operational Risk	3.9	1.7	2.8	10.92	□	□
6	The risk that an increase in raw material cost cuts our margins	Raw Material	4.0	3.0	1.5	6.00	□	□
7	The risk that fraudulant activity occurs in our organization	Financial Risk	2.5	2.9	3.0	7.50	□	□
8	The risk that a trough in the market occurs and decreases our client's propensity to buy	Economic Risk	2.5	1.7	2.5	6.25	□	□
9	The risk that a competing service emerges at a lower cost	Competition Risk	2.6	3.8	2.8	7.28	□	□





Risk that IT software fails causing an interruption in business operations, threatening the organizaiton's ability to sustain operations and provide essential services.

Indicate the perceived effectiveness of the existing control in place for this risk



Resolver User Conference 2016 > Impact/Likelihood/Ctrl Effectiveness > **Heatmap Report**

Rank	Risk	X	Y	X * Y
1	003 - **Theft of company property**	3.50	2.00	7.00
2	004 - **Theft of company's core IP**	1.50	4.00	6.00
3	006 - **Storefront vandalism**	3.50	1.50	5.25
4	007 - **Extortion**	2.00	2.50	5.00
5	008 - **Sexual assault**	2.50	2.00	5.00
6	005 - **Malicious destruction of company data**	2.00	2.50	5.00
7	001 - **Labour Unrest**	1.50	2.50	3.75
8	002 - **Flooding of key facility**	1.50	2.50	3.75

Legend:

Likelihood / Probability	Impact
1 Remote (0-20%)	**1** Minor (<2% EBiTDA)
2 Somewhat Likely (20-40%)	**2** Moderate (2%-15% EBiTDA)
3 Likely (40-60%)	**3** Major (15%-30% EBiTDA)
4 Very Likely (60-80%)	**4** Severe (30%-50% EBiTDA)

Meet Shayne Bates!

Shayne Bates interviews…..Shayne Bates

Corporate security: Managing risk across the security continuum

Shayne Bates explains the complicated world of Enterprise Security Risk Management

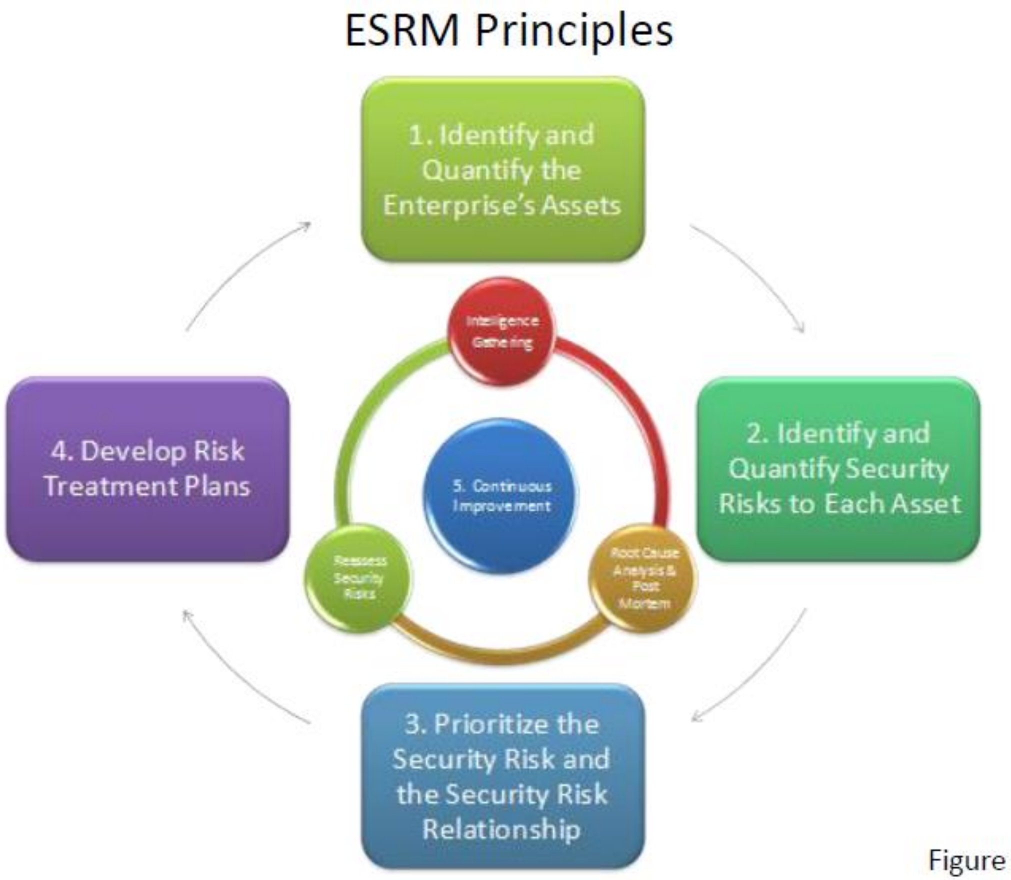
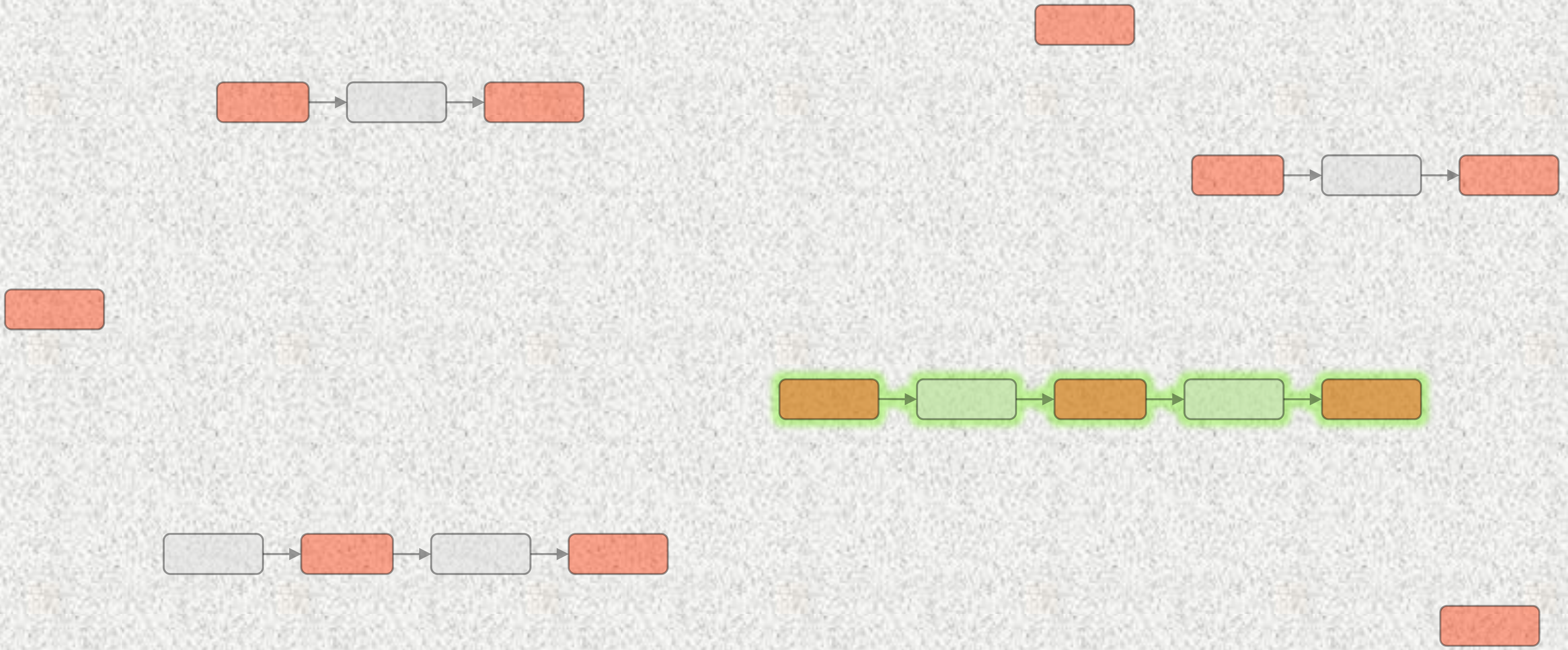
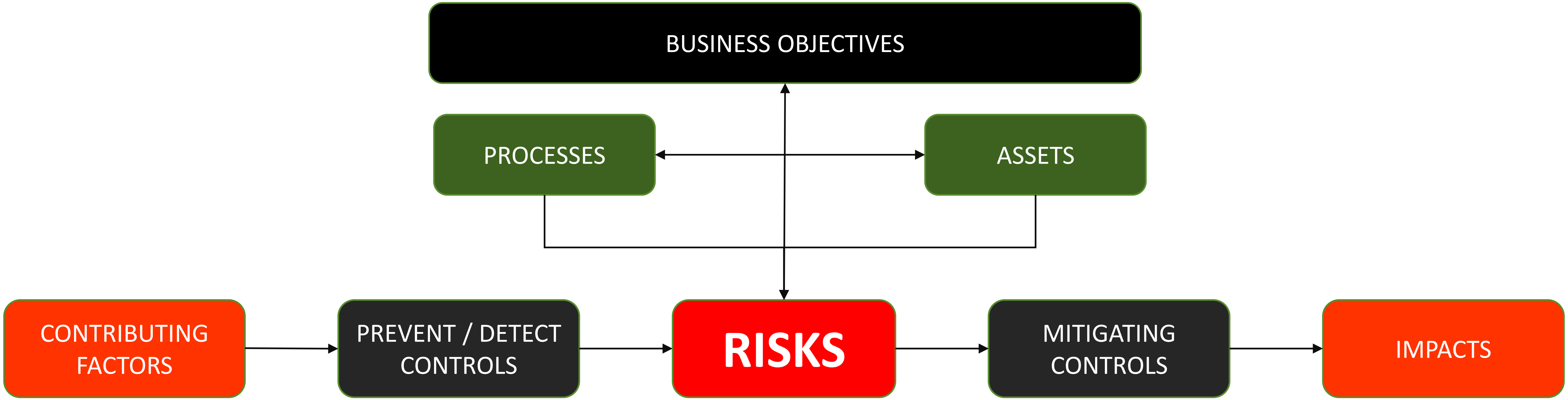

ESRM Principles
1. Identify and Quantify the Enterprise's Assets
2. Identify and Quantify Security Risks to Each Asset
3. Prioritize the Security Risk and the Security Risk Relationship
4. Develop Risk Treatment Plans
5. Continuous Improvement
Intelligence Gathering
Root Cause Analysis & Post Mortem
Reassess Security Risks

Figure 1

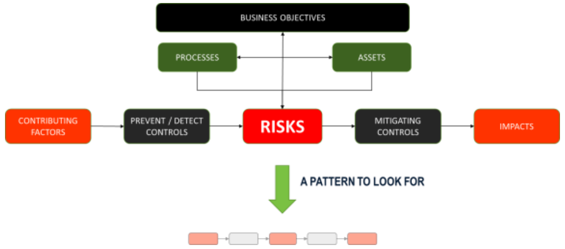
Risk Managed. Workshop – Day II
We dive into……

REAL LIFE - EVENTS OF ALL SORTS OCCUR





A PATTERN TO LOOK FOR


BUSINESS OBJECTIVES

PROCESSES

ASSETS

CONTRIBUTING FACTORS

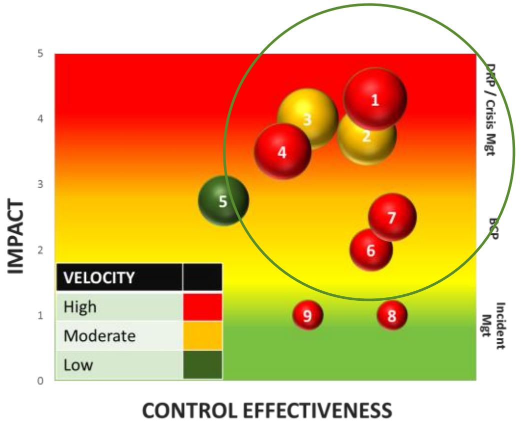
PREVENT / DETECT CONTROLS

RISKS

MITIGATING CONTROLS

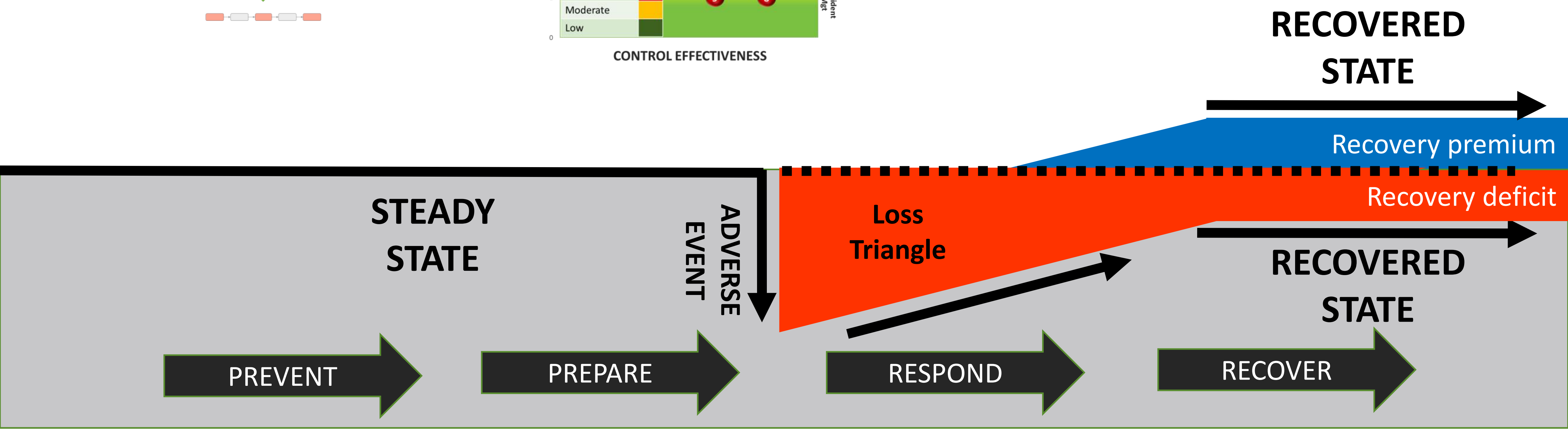
IMPACTS

A PATTERN TO LOOK FOR



VELOCITY	
High	🟥
Moderate	🟧
Low	🟩

1. Adopt a robust and integrated risk assessment approach
2. Detect and respond to events as they happen
3. Focus upon high velocity, high impact risks


RECOVERED STATE

Recovery premium

Recovery deficit

STEADY STATE

ADVERSE EVENT

Loss Triangle

RECOVERED STATE

PREVENT

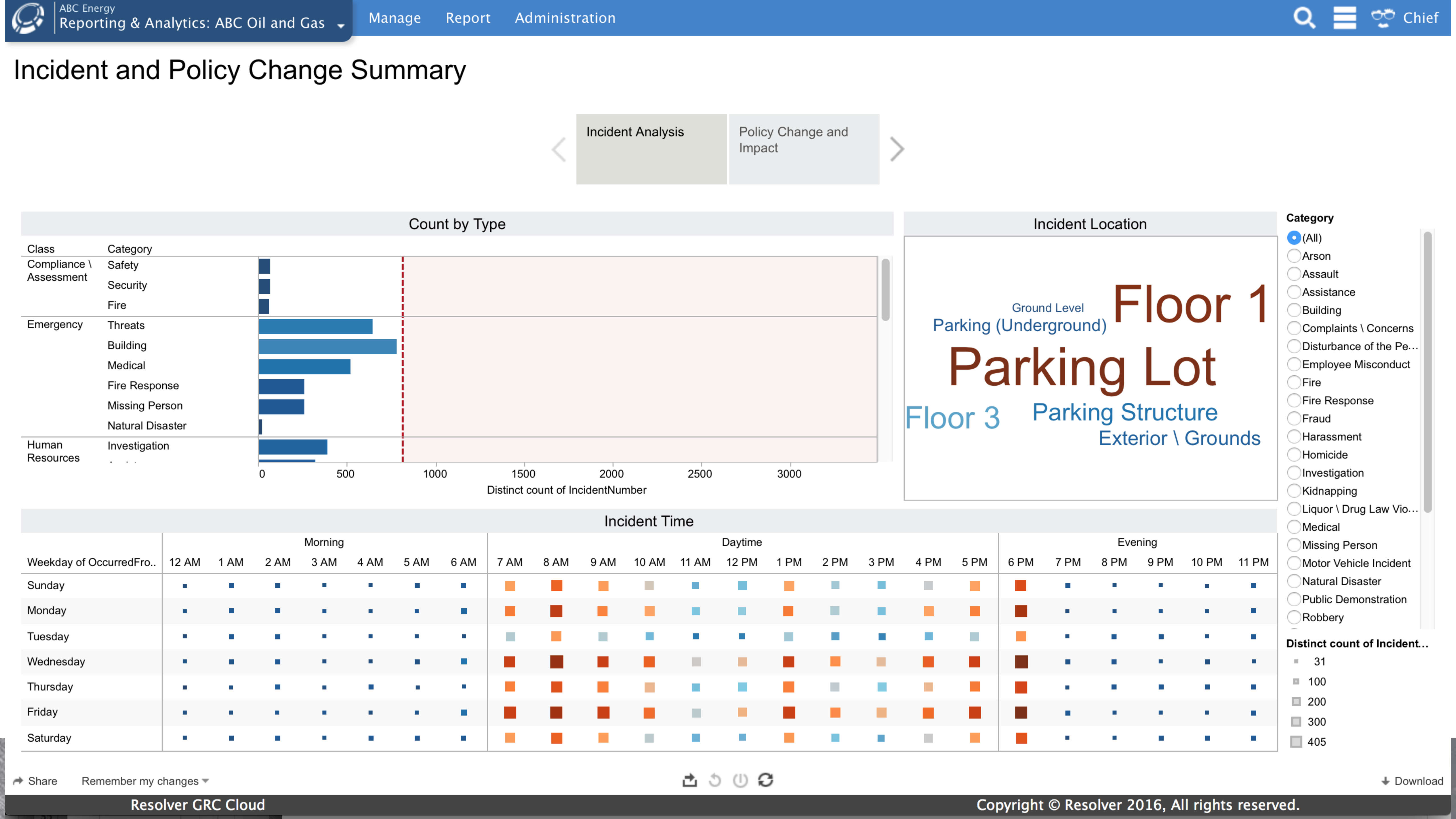
PREPARE

RESPOND

RECOVER

“hook into the bigger aggregators”

“Incident management tools Management Systems and PPM 2000 have helped him to manage physical and information security incidents. All these tools need to “hook into the bigger aggregators, the dashboard views of the world.”
Richard says that his company uses risk management software tools which helps manage governance, risk, & compliance”

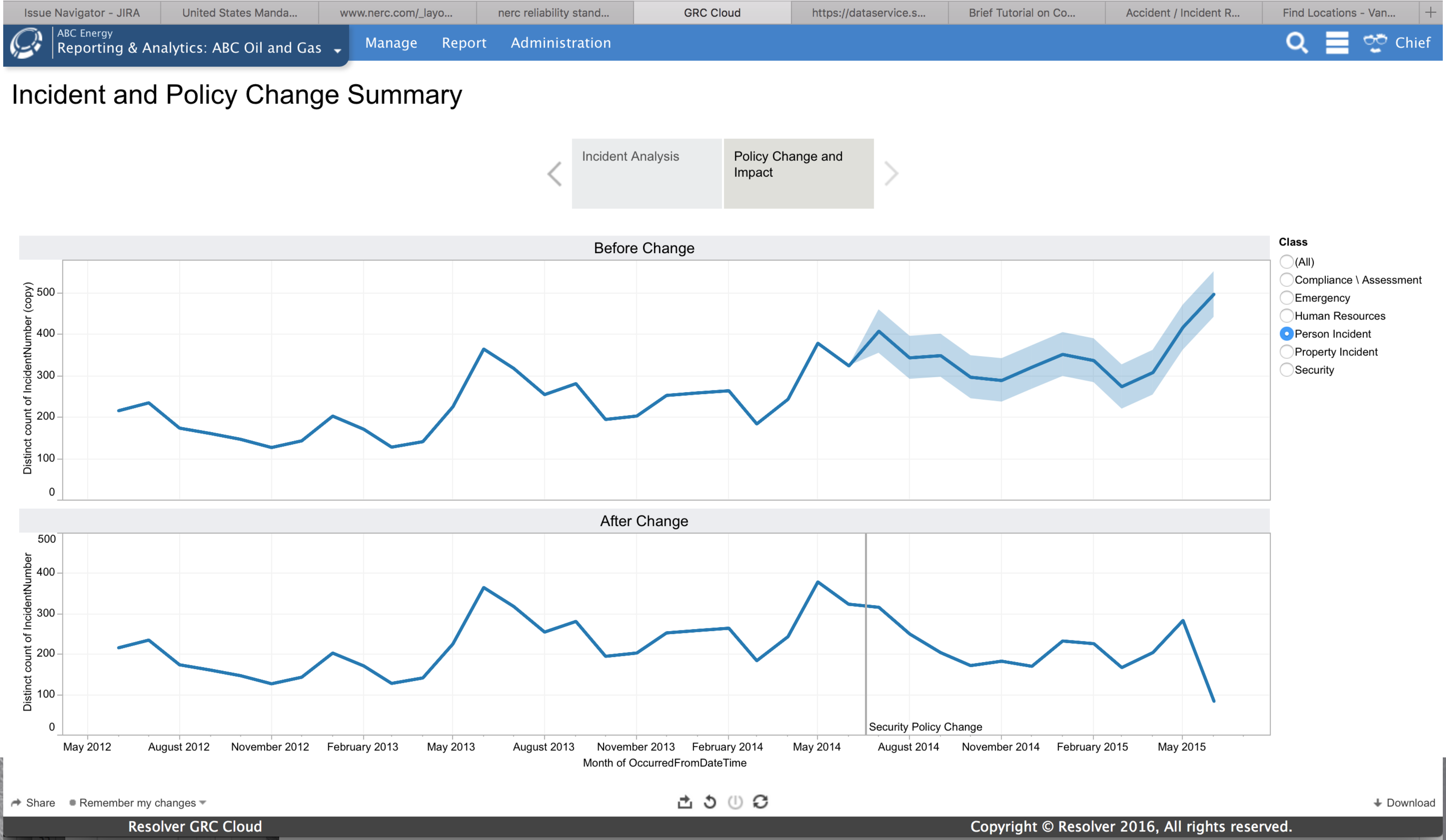


Incident and Policy Change Summary

Category

- ● (All)
- ○ Arson
- ○ Assault
- ○ Assistance
- ○ Building
- ○ Complaints \ Concerns
- ○ Disturbance of the Pe…
- ○ Employee Misconduct
- ○ Fire
- ○ Fire Response
- ○ Fraud
- ○ Harassment
- ○ Homicide
- ○ Investigation
- ○ Kidnapping
- ○ Liquor \ Drug Law Vio…
- ○ Medical
- ○ Missing Person
- ○ Motor Vehicle Incident
- ○ Natural Disaster
- ○ Public Demonstration
- ○ Robbery

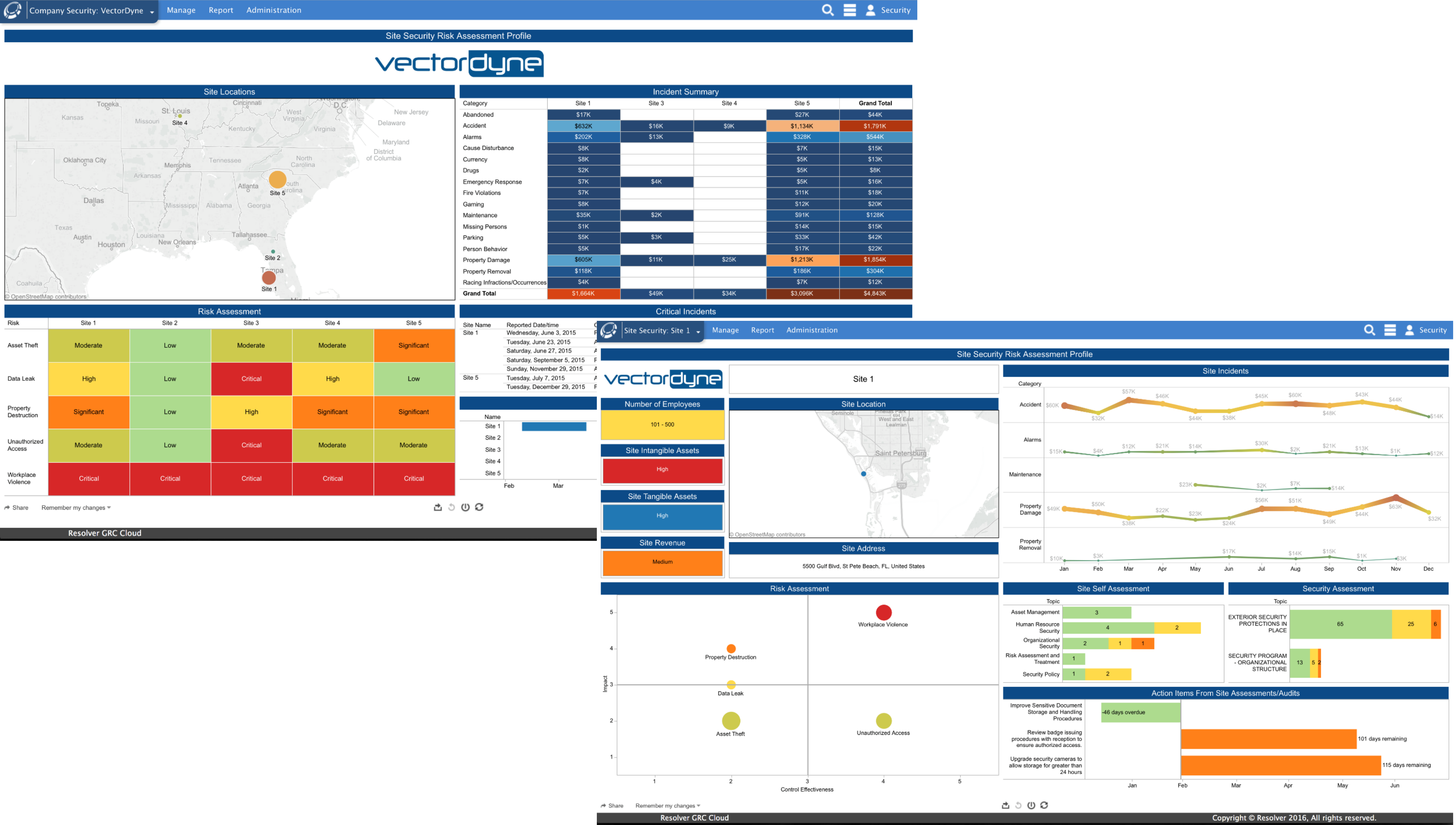
Resolver GRC Cloud



Incident and Policy Change Summary

Class

○ (All)
○ Compliance \ Assessment
○ Emergency
○ Human Resources
● Person Incident
○ Property Incident
○ Security



Site Security Risk Assessment Profile

Site Locations

Incident Summary

Category	Site 1	Site 3	Site 4	Site 5	Grand Total
Abandoned	$17K			$27K	$44K
Accident	$632K	$16K	$9K	$1,134K	$1,791K
Alarms	$202K	$13K		$328K	$544K
Cause Disturbance	$8K			$7K	$15K
Currency	$8K			$5K	$13K
Drugs	$2K			$5K	$8K
Emergency Response	$7K	$4K		$5K	$16K
Fire Violations	$7K			$11K	$18K
Gaming	$8K			$12K	$20K
Maintenance	$35K	$2K		$91K	$128K
Missing Persons	$1K			$14K	$15K
Parking	$5K	$3K		$33K	$42K
Person Behavior	$5K			$17K	$22K
Property Damage	$605K	$11K	$25K	$1,213K	$1,854K
Property Removal	$118K			$186K	$304K
Racing Infractions/Occurrences	$4K			$7K	$12K
Grand Total	$1,664K	$49K	$34K	$3,096K	$4,843K

Risk Assessment

Risk	Site 1	Site 2	Site 3	Site 4	Site 5
Asset Theft	Moderate	Low	Moderate	Moderate	Significant
Data Leak	High	Low	Critical	High	Low
Property Destruction	Significant	Low	High	Significant	Significant
Unauthorized Access	Moderate	Low	Critical	Moderate	Moderate
Workplace Violence	Critical	Critical	Critical	Critical	Critical

Critical Incidents

Site Name	Reported Date/time	C
Site 1	Wednesday, June 3, 2015	F
	Tuesday, June 23, 2015	A
	Saturday, June 27, 2015	A
	Saturday, September 5, 2015	F
	Sunday, November 29, 2015	A
Site 5	Tuesday, July 7, 2015	A
	Tuesday, December 29, 2015	F

Site Security Risk Assessment Profile

Site 1

Number of Employees

101 - 500

Site Intangible Assets

High

Site Tangible Assets

High

Site Revenue

Medium

Site Location

Site Address

5500 Gulf Blvd, St Pete Beach, FL, United States

Site Incidents

Risk Assessment

Site Self Assessment

Security Assessment

Topic
EXTERIOR SECURITY PROTECTIONS IN PLACE
65
25
6
SECURITY PROGRAM - ORGANIZATIONAL STRUCTURE
13
5
2

Action Items From Site Assessments/Audits

Improve Sensitive Document Storage and Handling Procedures
-46 days overdue
Review badge issuing procedures with reception to ensure authorized access.
101 days remaining
Upgrade security cameras to allow storage for greater than 24 hours
115 days remaining
Jan
Feb
Mar
Apr
May
Jun
Share
Remember my changes
Resolver GRC Cloud

Obsessing Over Raw Numbers

“One of the hurdles we face in the security industry is that while the processes and systems used to collect and manage data have improved tremendously, there has been comparatively little attention given to the analysis and effective communication of that data. The unfortunate reality is that most of us have put far too much stock in flashy dials and graphs that communicate little, and what they do communicate, they do so poorly….”

“Whether it’s determining the effectiveness of new security measures or identifying nuisance alarms, we must have enough context to differentiate what is normal fluctuation (i.e. noise) from true trends and outliers (i.e. signals)”

FAKE CHART 1

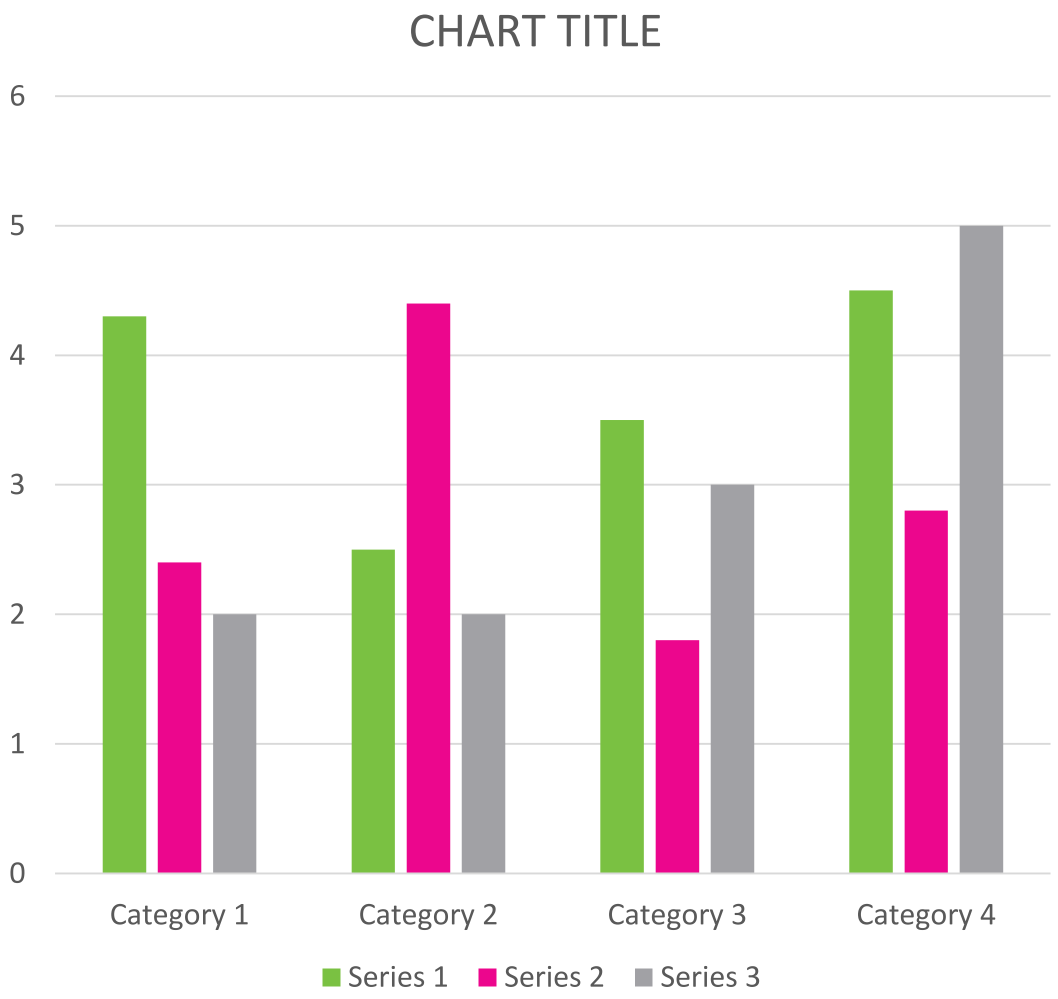


CHART TITLE
6
5
4
3
2
1
0
Category 1
Category 2
Category 3
Category 4
🟩 Series 1
🟥 Series 2
⬜ Series 3

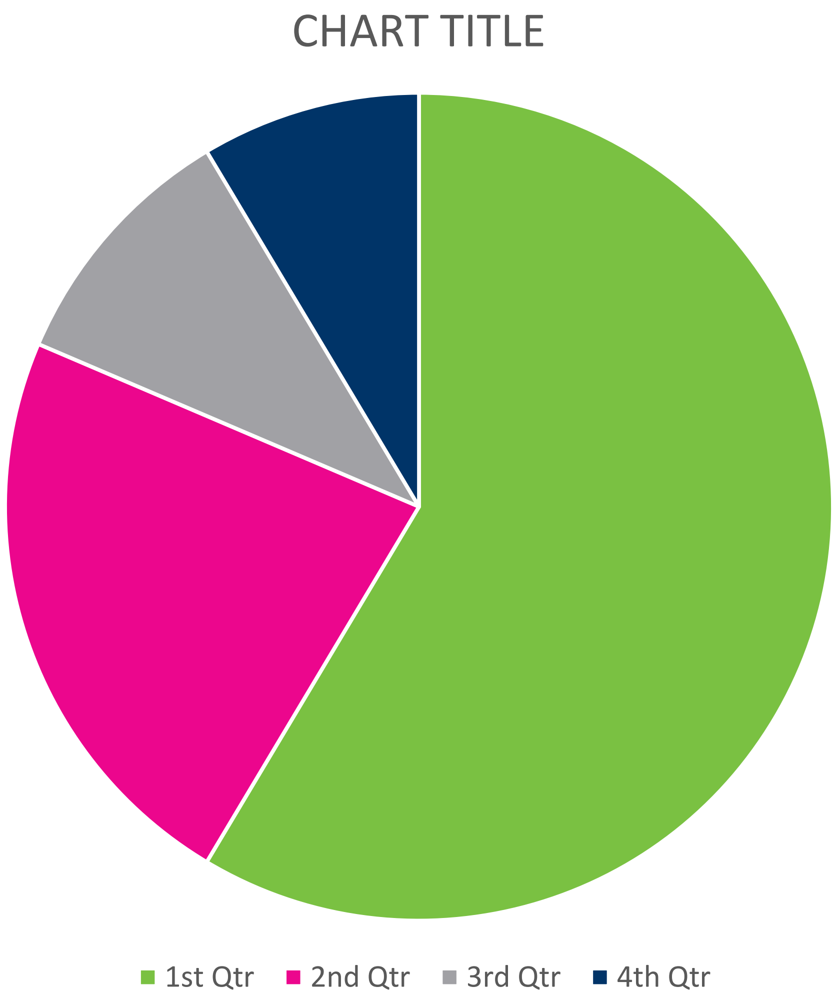
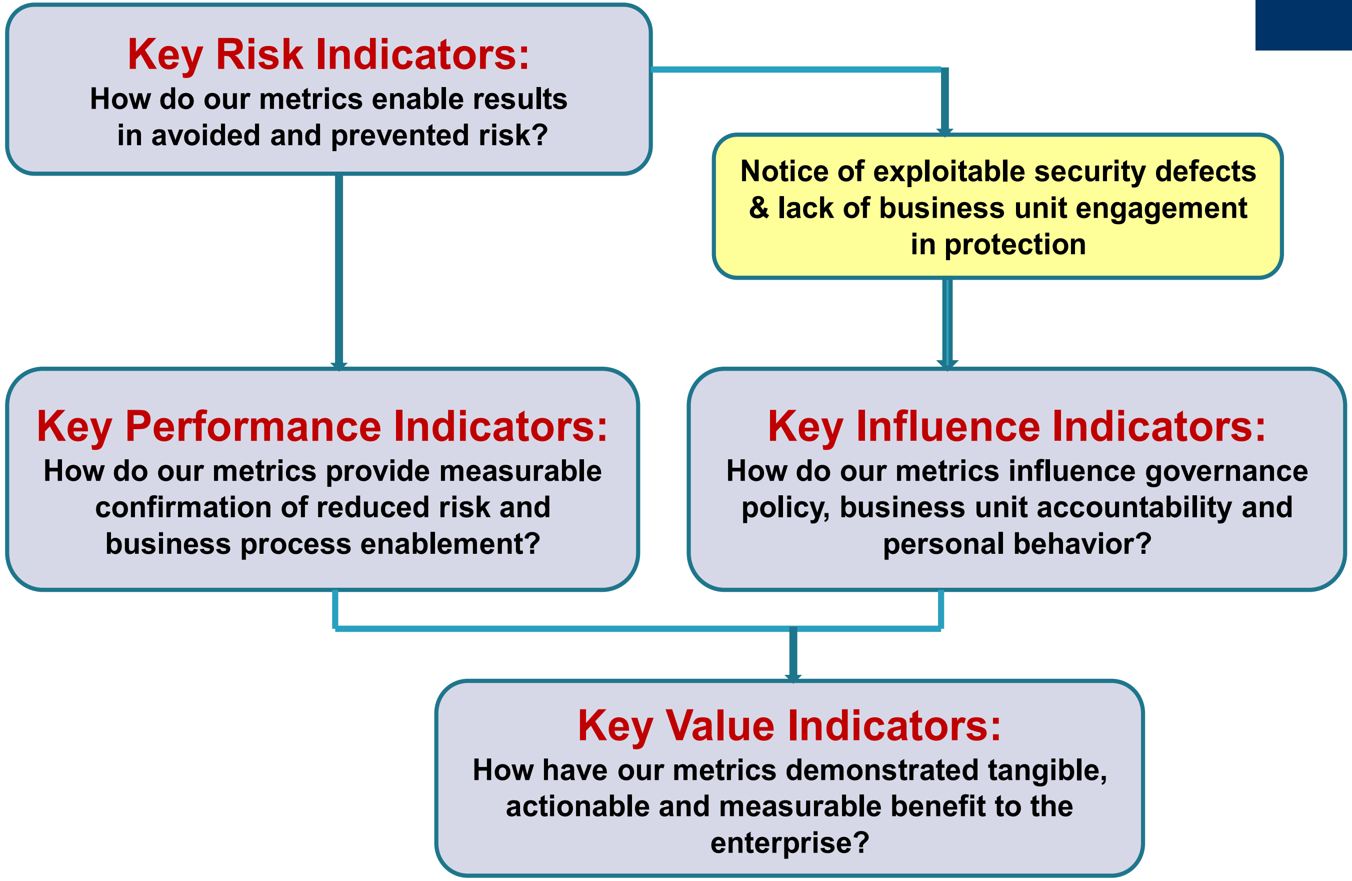


CHART TITLE
🟩 1st Qtr
🟥 2nd Qtr
⬜ 3rd Qtr
🟦 4th Qtr

Security’s Metric Products

George Campbell
Security Executive Council



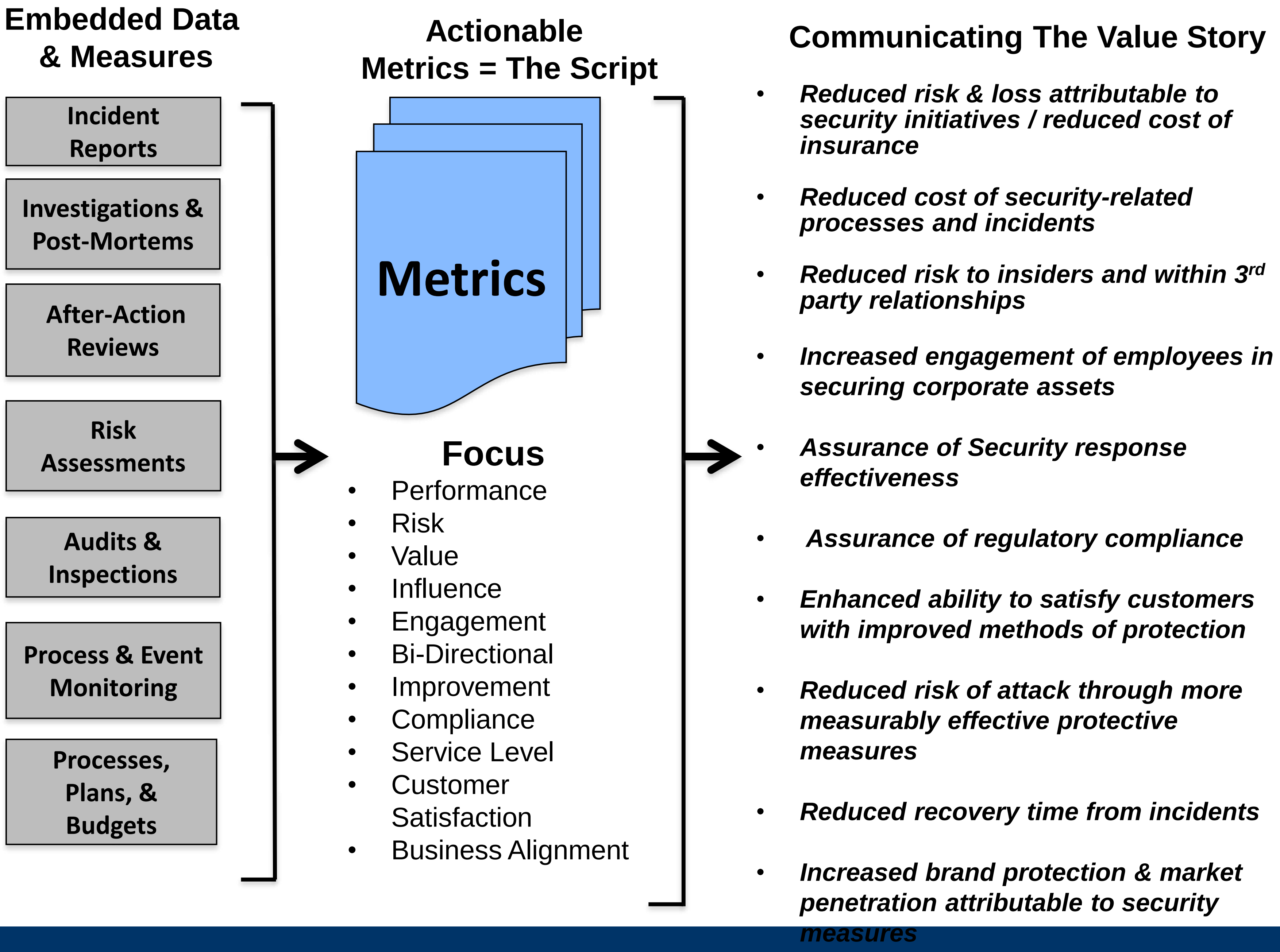
Key Risk Indicators:
How do our metrics enable results in avoided and prevented risk?

Notice of exploitable security defects & lack of business unit engagement in protection

Key Performance Indicators:
How do our metrics provide measurable confirmation of reduced risk and business process enablement?

Key Influence Indicators:
How do our metrics influence governance policy, business unit accountability and personal behavior?

Key Value Indicators:
How have our metrics demonstrated tangible, actionable and measurable benefit to the enterprise?



Embedded Data & Measures

- Incident Reports
- Investigations & Post-Mortems
- After-Action Reviews
- Risk Assessments
- Audits & Inspections
- Process & Event Monitoring
- Processes, Plans, & Budgets

Actionable Metrics = The Script

Metrics

Focus

- Performance
- Risk
- Value
- Influence
- Engagement
- Bi-Directional
- Improvement
- Compliance
- Service Level
- Customer Satisfaction
- Business Alignment

Communicating The Value Story

- *Reduced risk & loss attributable to security initiatives / reduced cost of insurance*
- *Reduced cost of security-related processes and incidents*
- *Reduced risk to insiders and within 3rd party relationships*
- *Increased engagement of employees in securing corporate assets*
- *Assurance of Security response effectiveness*
- *Assurance of regulatory compliance*
- *Enhanced ability to satisfy customers with improved methods of protection*
- *Reduced risk of attack through more measurably effective protective measures*
- *Reduced recovery time from incidents*
- *Increased brand protection & market penetration attributable to security measures*

RISK, INCIDENTS. Same Sand, Different Castles