Canadian Security
THE PUBLICATION FOR PROFESSIONAL SECURITY MANAGEMENT

:RESOLVER

RISK-incidents:
same playground, different castles

RISK & INCIDENTS: SAME SAND – Different CASTLES

RISK & INCIDENTS: SAME SAND – SAME CASTLES – DIFFERENT PROPERTIES

RISK!

Likel ihood!

Impact ?

AT
YOUR OWN
RISK

AT YOUR OWN RISK

AT
YOUR OWN
RISK

LOW RISK
HIGH RISK
NO RISK

LOW RISK
HIGH RISK
NO RISK

RISK
REWARD

LOW RISK
HIGH RISK
NO RISK

RISK
REWARD

R
I
S
K

LOW RISK
HIGH RISK
NO RISK

RISK
REWARD

R
I
S
K

AVOID
REDUCE
RISK
SFER

identification
probability
cost
scope
risk
strategy
index
retention
control
avoidance
business
event
context
sharing
method
prioritization
reduction
management
evaluation
opportunity
uncertain
resource
monitor
objective
treatment
implementation
process
plan
impact
solution
assessment
standard
knowledge
project
analysis

RISK
MANAGEMENT
external
internal
triggers
hazards
dynamic
mapping
control
transfer
retention
constraints
causes
natural
carrier
scope
review
source
BUSINESS
method
PRIORITIZE
DETERMINE
prevention
share
REDUCE
liability
threats
outsource
assets
frequency
scenario
opportunity
cost
monitor
agreement
IDENTIFY
RESOURCE
index
STRATEGY
optimize
data
practical
systematic
profit
EVALUATE
uncertainty
events
legal
responsive
avoid
index
ANALYSIS
change
dangers
coverage
PROCESS
stakeholders
design
cost
eliminate
subrogation
STANDARDS
human
factor
fire
security
knowledge
mitigation
insure
environmental
dimensions
ASSESS
transparent
probability
accident
control
ISO
implementation
financing
impact
financing
severity
options
budget
PLAN
inclusive

RISK
MANAGEMENT
PROJECT
LOSS
RESOURCES
FORMULA
PROBLEM
TERM
TRANSFER
AVOIDANCE
DIFFICULT
BENEFIT
AVOID
INSURED
LARGE
SOFTWARE
EFFECTIVE
PUBLIC
CITATION
EFFECT
GREATER
PLANNING
TECHNIQUES
RETENTION
NATURAL
SHARING
THREAT
DIFFERENT
TAXONOMY
HAZARD
AVAILABLE
PLANS
IMPACT
SEVERAL
COMMUNICATION
PREVENTION
LEVEL
OCCUR
VALUE
CASE
COMPOSITE
STAGE
SECURITY
EVENTS
PARTICULAR
LOWER
OBJECTIVES
FACTORS
POSSIBLE
INDUSTRY
FINANCIAL
COMPANY
SAFETY
DEVELOPMENT
REDUCTION
NEEDED
MITIGATION
MAIN
OCCURRING
TAKE
IMPLEMENTATION
ANALYSIS
OPERATIONAL
IDENTIFICATION
COST
ORGANIZATION
CHANGES
MOST
TIE
MARKET
PROCESSES
NEEDS
ACCEPTED
TRAFFIC
ASSESS
DEFINED
PROCESS
EVENT
INSURANCE
CONTROLS
DECISIONS
BUSINESS
ASSESSMENT
APPROPRIATE
SPECIFIC
ACTIVITIES
OCCURRENCE
POTENTIAL
CONTROL
LEGAL
ENVIRONMENT
TIME
ACCORDING
DEAL
ESTIMATE
INVOLVES
PRIMARY
FOLLOWING
POLICY
PRACTICE
TERMS
OFFSHORE
ASSETS
MAKING
ENTERPRISE
INFORMATION
PROBABILITY
NEGATIVE
CONSEQUENCES
SCHEDULE
IDENTIFIED
CAUSE
SOURCES
ESTABLISHING
BEST
KNOWLEDGE
LIABILITY
THREATS
BASED
MANAGING
AREAS
ASSESSED
CAPACITY
INCREASE
RELATED
PART
MEASURES
STANDARD
INTERNATIONAL
DECISION
METHOD
TECHNOLOGY
PLAN
HIGH
APPLIED
DIAGRAMS
SOURCE
SIMPLY
UNCERTAINTY
EXTERNAL
LOSSES
OCCURS
CONTEXT
ACCEPT
HANDLED
GROUP
KNOWN
MAJOR
CREATE
IMPACTS

What Does It All Mean?

Event, Impact, Indicators, Loss, Consequences, threats, events, cause, probability, ranges, good, outcomes, poor, positive, negative, trends, alert, avoid, occurrence, likelihood, severity, uncertainty, measures, analysis…

What Does It All Mean?

Event, Impact, Indicators, Loss, Consequences, threats, events, cause, probability, ranges, good, outcomes, poor, positive, negative, trends, alert, avoid, occurrence, likelihood, severity, uncertainty, measures, analysis…

What Does It All Mean?

Event, Impact, Indicators, Loss, Consequences, threats, events, cause, probability, ranges, good, outcomes, poor, positive, negative, trends, alert, avoid, occurrence, likelihood, comparative, severity, uncertainty, measures, analysis…

What Does It All Mean?

Event, Impact, Indicators, Loss, Consequences, threats, events, cause, probability, ranges, good, outcomes, poor, positive, negative, trends, alert, avoid, occurrence, likelihood, severity, uncertainty, measures, analysis...

INDICATORS

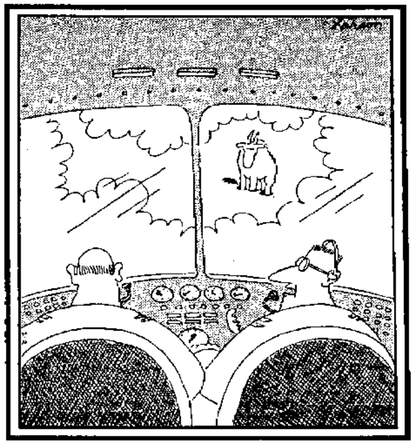
DATA VISUALIZATION

WHY INDICATORS ARE IMPORTANT

WHY VISUAL INDICATORS ARE IMPORTANT

DATA VISUALIZATION

WHY INDICATORS ARE IMPORTANT



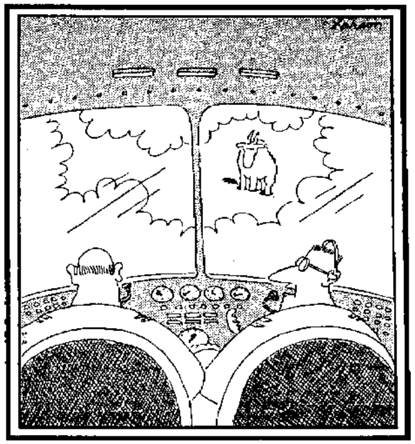
"Say . . .

What's a
mountain goat
doing way up
here in a
cloud bank?"

WHY VISUAL INDICATORS ARE IMPORTANT

DATA VISUALIZATION

WHY INDICATORS ARE IMPORTANT



"Say . . .

What's a
mountain goat
doing way up
here in a
cloud bank?"

WHY VISUAL INDICATORS ARE IMPORTANT

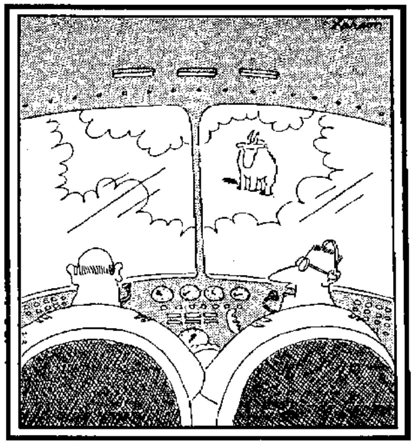
CAUTION
THIS SIGN HAS
SHARP EDGES
DO NOT TOUCH THE EDGES OF THIS SIGN
ALSO, THE BRIDGE IS OUT AHEAD

DATA VISUALIZATION

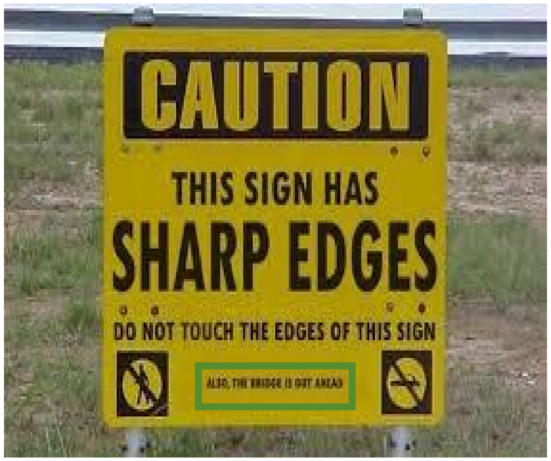
WHY INDICATORS ARE IMPORTANT

"Say . . .

What's a mountain goat doing way up here in a cloud bank?"



WHY VISUAL INDICATORS ARE IMPORTANT


CAUTION
THIS SIGN HAS
SHARP EDGES
DO NOT TOUCH THE EDGES OF THIS SIGN
ALSO, THE BRIDGE IS OUT AHEAD

What's the Value Story?

What's the value story?

Could you possibly expand on "Oops, looks like something bad happened"?

What’s the value story?

Could you possibly expand on “Oops, looks like something bad happened”?

..Sorry, explain to me how giving you $3.5 million $$ is ‘good’.

Risk Management: The Primary Function of Security

Assess, manage and mitigate risk using existing information.

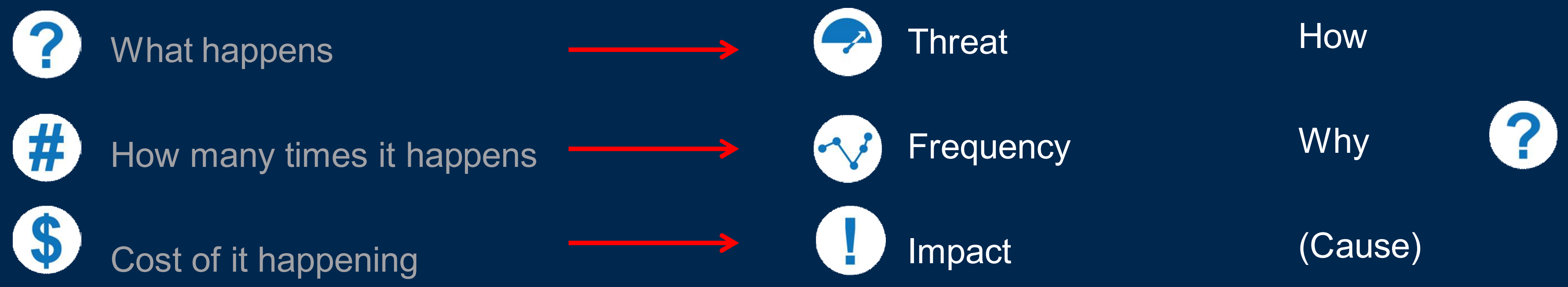
? What happens → Threat

How many times it happens → Frequency

$ Cost of it happening → ! Impact

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

Tornados
Hurricanes
Storms
Floods
Earthquakes

Human Driven Events

Thefts
Assaults
Murders
Bombs
Frauds

Uncontrolled Events

Fires/Explosions
Surrounded Event
Personal Injury Accidents
Industrial Accidents
System Failures

WHAT WE KNOW ABOUT INCIDENTS

INCIDENT TYPES:

Natural Events

Tornados
Hurricanes
Storms
Floods
Earthquakes

Human Driven Events

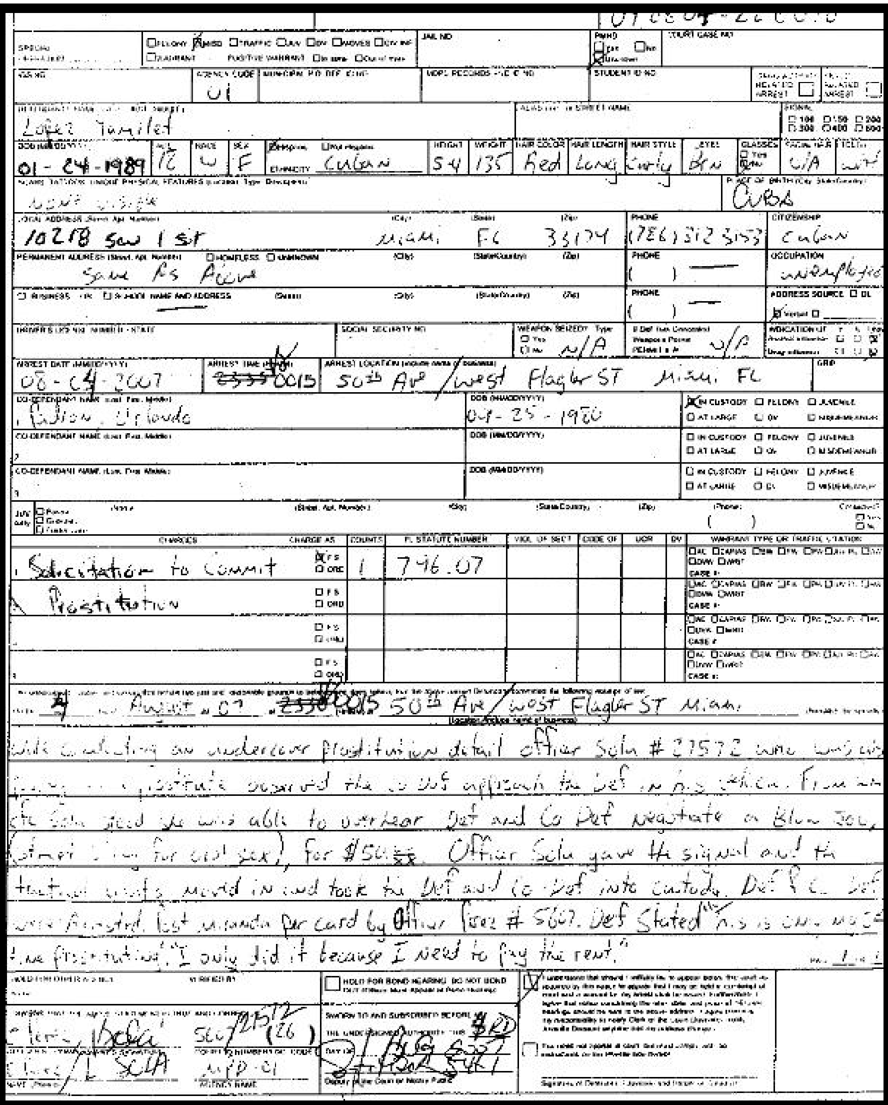
Thefts
Assaults
Murders
Bombs
Frauds

Uncontrolled Events

Fires/Explosions
Surrounded Event
Personal Injury Accidents
Industrial Accidents
System Failures

IT HR Risk Management Legal Security Ethics Compliance Safety Environment

Incidents and Events at Departmental Level



07-22-04-22[illegible]

SPECIAL [illegible] □ FELONY ☒ MISD □ TRAFFIC □ JUV □ DV □ MOVES □ CIV INF
□ FUGITIVE WARRANT □ [illegible] □ [illegible]
JAIL NO
PWND □ Yes □ No ☒ Unknown
COURT CASE NO

[illegible] NO
AGENCY CODE: 01
MUNICIPAL P.D. DEF. [illegible]
MDPD RECORDS [illegible] NO
STUDENT ID NO
[illegible] RELATED ARREST □
[illegible] RELATED ARREST □

DEFENDANT NAME (Last, First, Middle): Lopez Yamilet
ALIAS [illegible] STREET NAME
[illegible] □ 100 □ 150 □ 200 □ 300 □ 400 □ 500

DOB (MM/DD/YYYY)	AGE	RACE	SEX	ETHNICITY	HEIGHT	WEIGHT	HAIR COLOR	HAIR LENGTH	HAIR STYLE	EYES	GLASSES	FACIAL HAIR	TEETH
01-24-1989	18	W	F	☒ Hispanic □ Not Hispanic Cuban	5 4	135	Red	Long	Curly	Brn	□ Yes ☒ No	N/A	wht

SCARS, TATTOOS, UNIQUE PHYSICAL FEATURES (Location, Type, Description): none visible
PLACE OF BIRTH (City, State/Country): CUBA

LOCAL ADDRESS (Street, Apt. Number): 10218 sw 1 st
(City): Miami (State): FL (Zip): 33174
PHONE: (786) 312 3153
CITIZENSHIP: cuban

PERMANENT ADDRESS (Street, Apt. Number) □ HOMELESS □ UNKNOWN: same As Above
(City) (State/Country) (Zip)
PHONE: ( ) —
OCCUPATION: unemployed

□ BUSINESS □ SCHOOL NAME AND ADDRESS: —
(Street) (City) (State/Country) (Zip)
PHONE: ( ) —
ADDRESS SOURCE □ DL ☒ Verbal □

DRIVER'S LICENSE NUMBER / STATE: N
SOCIAL SECURITY NO
WEAPON SEIZED? Type □ Yes □ No N/A
If Def. has Concealed Weapons Permit [illegible]: N/A
INDICATION OF: Alcohol influence □ □ ☒ Drug influence □ □ ☒

ARREST DATE (MM/DD/YYYY): 08-04-2007
ARREST TIME (HHMM): ~~2335~~ 0015
ARREST LOCATION (include name of business): 50th Ave / west Flagler ST Miami FL
GRID

CO-DEFENDANT NAME (Last, First, Middle)	DOB (MM/DD/YYYY)	
1 Colon, Orlando	04-25-1980	☒ IN CUSTODY □ FELONY □ JUVENILE □ AT LARGE □ DV □ MISDEMEANOR
2		□ IN CUSTODY □ FELONY □ JUVENILE □ AT LARGE □ DV □ MISDEMEANOR
3		□ IN CUSTODY □ FELONY □ JUVENILE □ AT LARGE □ DV □ MISDEMEANOR

JUV Notify □ Parent □ Guardian □ [illegible] Name (Street, Apt. Number) (City) (State/Country) (Zip) (Phone) ( ) Contacted? □ Yes □ No

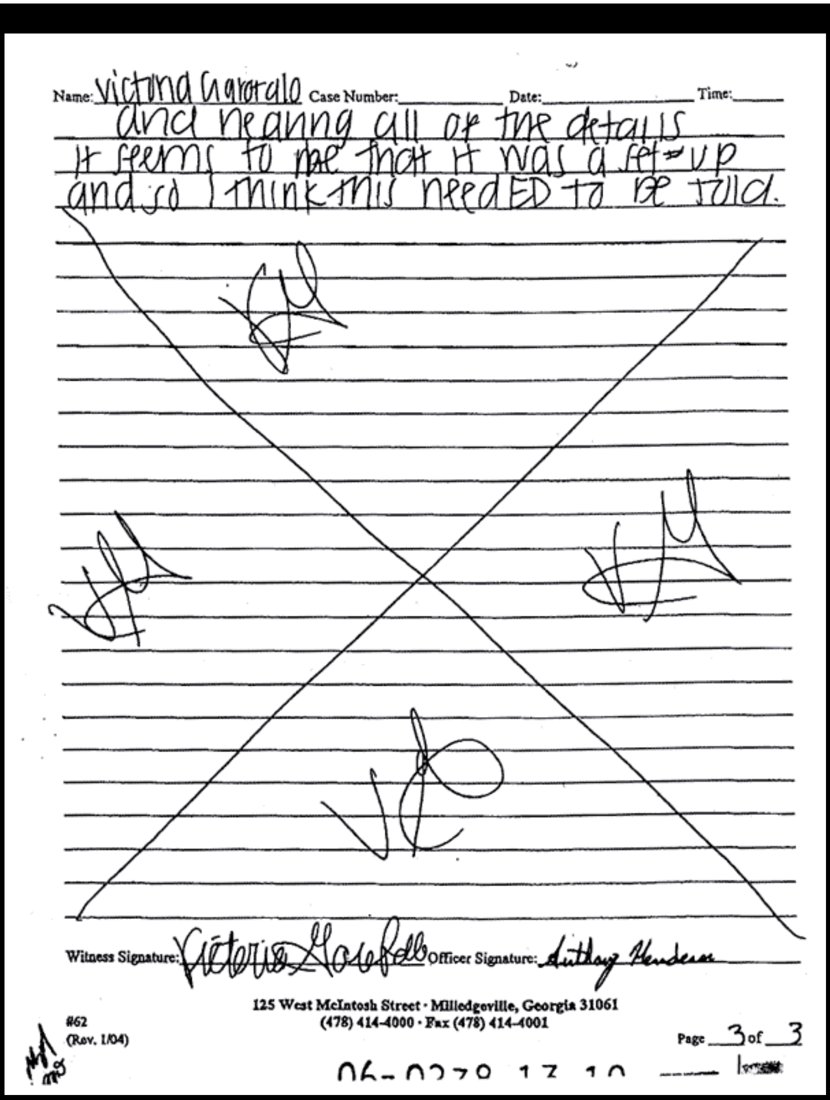
CHARGES	CHARGE AS	COUNTS	FL STATUTE NUMBER	VIOL OF SECT	CODE OF	UCR	DV	WARRANT TYPE OR TRAFFIC CITATION
1 Solicitation to Commit	☒ F.S. □ ORD	1	796.07					□ AC □ CAPIAS □ [illegible] □ [illegible] □ [illegible] □ [illegible] □ [illegible] □ DW □ WRIT CASE #:
Prostitution	□ F.S. □ ORD							□ AC □ CAPIAS □ [illegible] □ [illegible] □ [illegible] □ [illegible] □ [illegible] □ DW □ WRIT CASE #:
	□ F.S. □ ORD							□ AC □ CAPIAS □ [illegible] □ [illegible] □ [illegible] □ [illegible] □ [illegible] □ DW □ WRIT CASE #:
4	□ F.S. □ ORD							□ AC □ CAPIAS □ [illegible] □ [illegible] □ [illegible] □ [illegible] □ [illegible] □ DW □ WRIT CASE #:

The undersigned [illegible] that he/she has just and reasonable grounds to believe, and does believe, that the above named Defendant committed the following violation of law:
On the 4 day of August, 07, at ~~2330~~ 0015 (hours) at 50th Ave / west Flagler ST Miami (Location/include name of business)

While conducting an undercover prostitution detail officer Sola #27572 who was [illegible] [illegible] [illegible] prostitute observed the co def approach the Def in his vehicle. From [illegible] the Sola [illegible] she was able to overhear Def and Co Def negotiate a Blow Job, (street [illegible] for oral sex), for $50.00. Officer Sola gave the signal and the tactical units moved in and took the Def and Co Def into custody. Def & Co Def were Arrested [illegible] miranda per card by Officer [illegible] #5607. Def stated "this is [illegible] the prostituting," "I only did it because I need to pay the rent."

Page 1 of [illegible]

HOLD FOR OTHER AGENCY [illegible] VERIFIED BY
□ HOLD FOR BOND HEARING. DO NOT BOND [illegible]
☒ I understand that should I willfully fail to appear before the court as required by this notice to appear that I may be held in contempt of court [illegible]
□ [illegible]
SWORN TO AND SUBSCRIBED BEFORE ME, THE UNDERSIGNED AUTHORITY THIS 3RD DAY OF [illegible]
Officer Sola 27572
5607 (26)
COURT ID NUMBER [illegible]
Office / L Sola
MPD-01
NAME (Print) / AGENCY NAME
Deputy [illegible] Clerk or Notary Public
Signature of Defendant / Juvenile and Parent or Guardian



Name: Victoria Garofalo Case Number:________ Date:________ Time:____

and hearing all of the details
it seems to me that it was a set-up
and so I think this needED to be told.

Witness Signature: Victoria Garofalo Officer Signature: Anthony Henderson

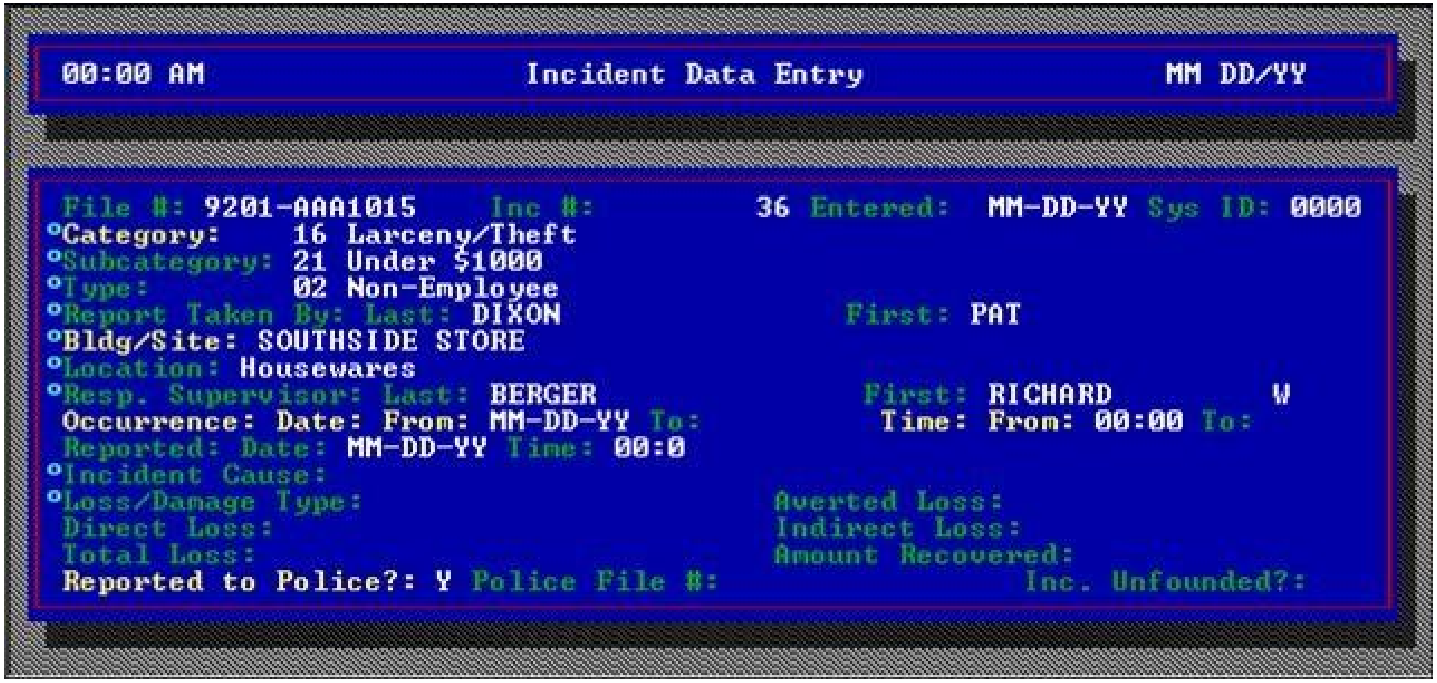
125 West McIntosh Street · Milledgeville, Georgia 31061
(478) 414-4000 · Fax (478) 414-4001

#62
(Rev. 1/04)

Page 3 of 3

06-0270 13 10

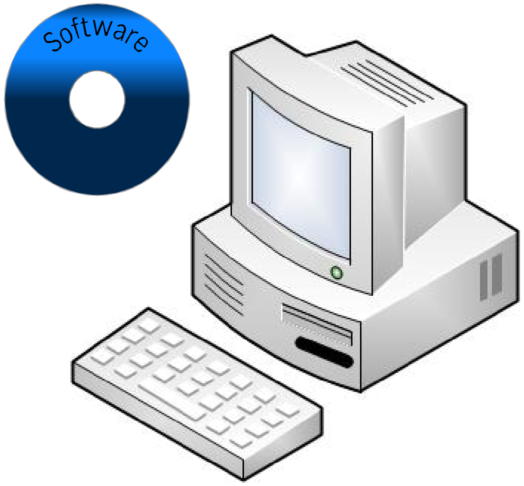
REPORTING

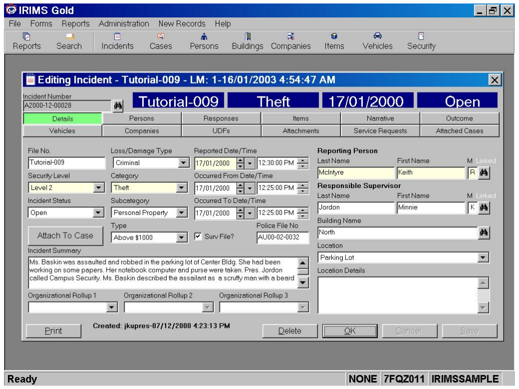


```
 00:00 AM                    Incident Data Entry                    MM DD/YY

 File #: 9201-AAA1015     Inc #:        36 Entered:  MM-DD-YY Sys ID: 0000
°Category:     16 Larceny/Theft
°Subcategory: 21 Under $1000
°Type:         02 Non-Employee
°Report Taken By: Last: DIXON               First: PAT
°Bldg/Site: SOUTHSIDE STORE
°Location: Housewares
°Resp. Supervisor: Last: BERGER              First: RICHARD          W
 Occurrence: Date: From: MM-DD-YY To:          Time: From: 00:00 To:
 Reported: Date: MM-DD-YY Time: 00:0
°Incident Cause:
°Loss/Damage Type:                         Averted Loss:
 Direct Loss:                              Indirect Loss:
 Total Loss:                               Amount Recovered:
 Reported to Police?: Y Police File #:                  Inc. Unfounded?:
```

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

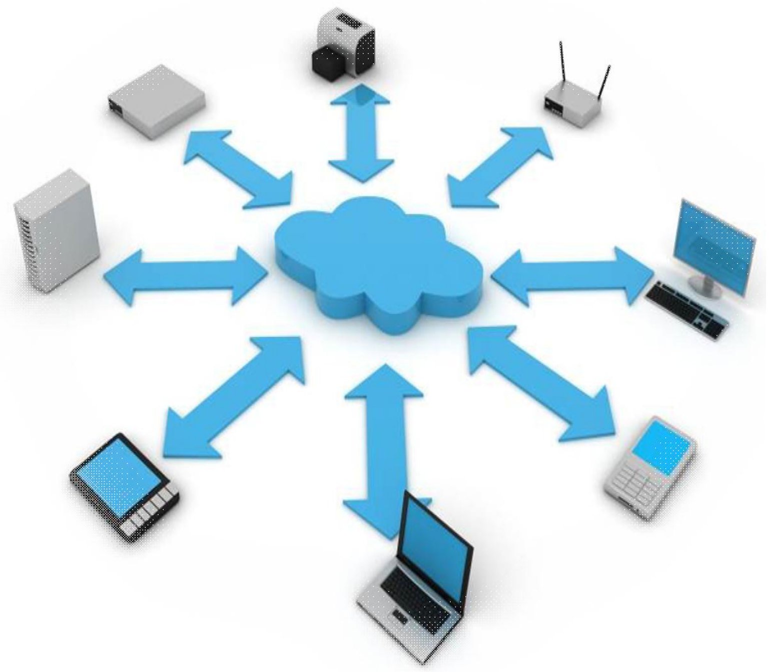
Location Details:

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

Ready | **NONE** | **7FQZ011** | **IRIMSSAMPLE**

COMPUTING THE NEW WAY

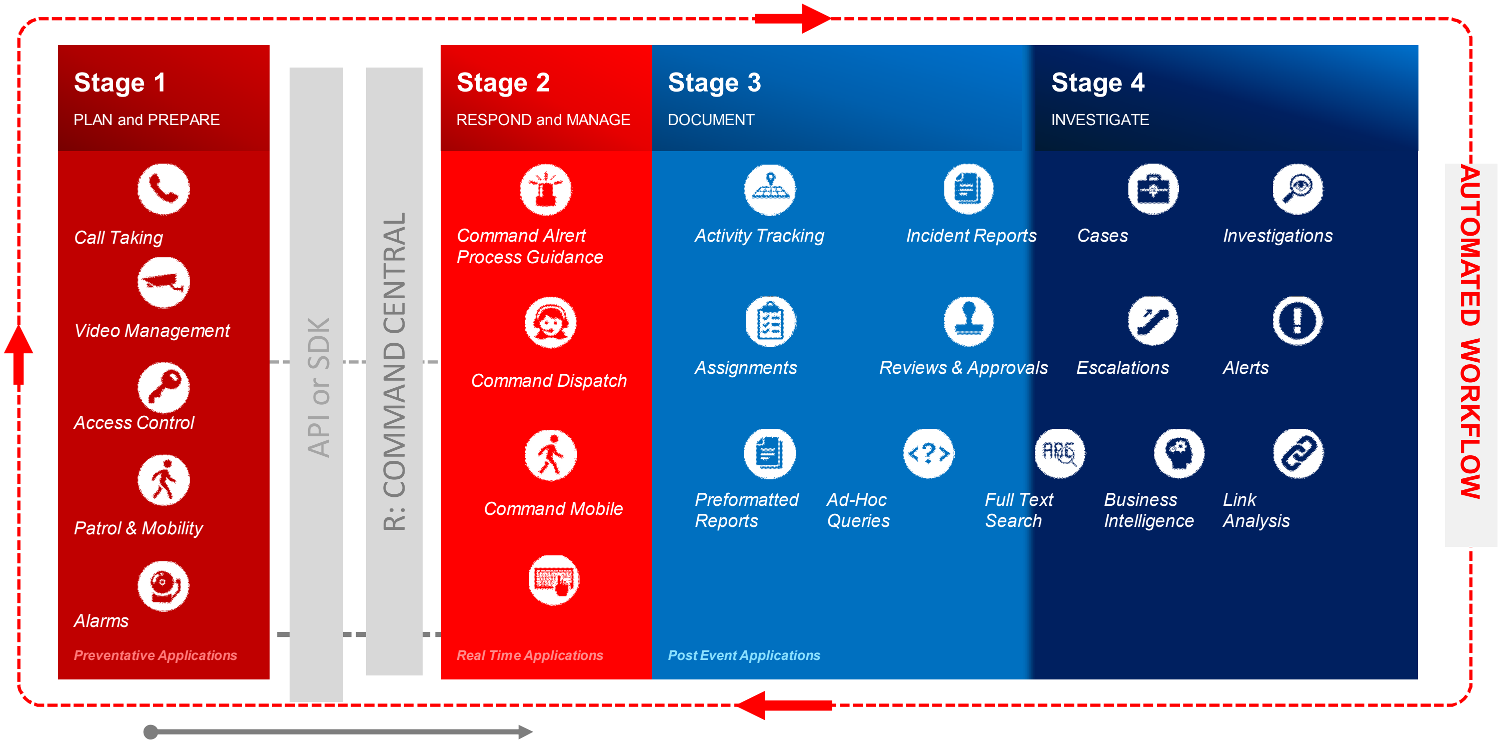
- Integration & Connected Systems
- Internet Based Programs
- Data & software in cloud
- Mobility
- IoT – Big Data



INTEGRATED INCIDENT MANAGEMENT

Interact. Communicate. Integrate

Connecting Data, Systems and People



Stage 1
PLAN and PREPARE

Call Taking

Video Management

Access Control

Patrol & Mobility

Alarms

Preventative Applications

API or SDK

R: COMMAND CENTRAL

Stage 2
RESPOND and MANAGE

Command Alert
Process Guidance

Command Dispatch

Command Mobile

Real Time Applications

Stage 3
DOCUMENT

Activity Tracking

Incident Reports

Assignments

Reviews & Approvals

Preformatted Reports

Ad-Hoc Queries

Full Text Search

Post Event Applications

Stage 4
INVESTIGATE

Cases

Investigations

Escalations

Alerts

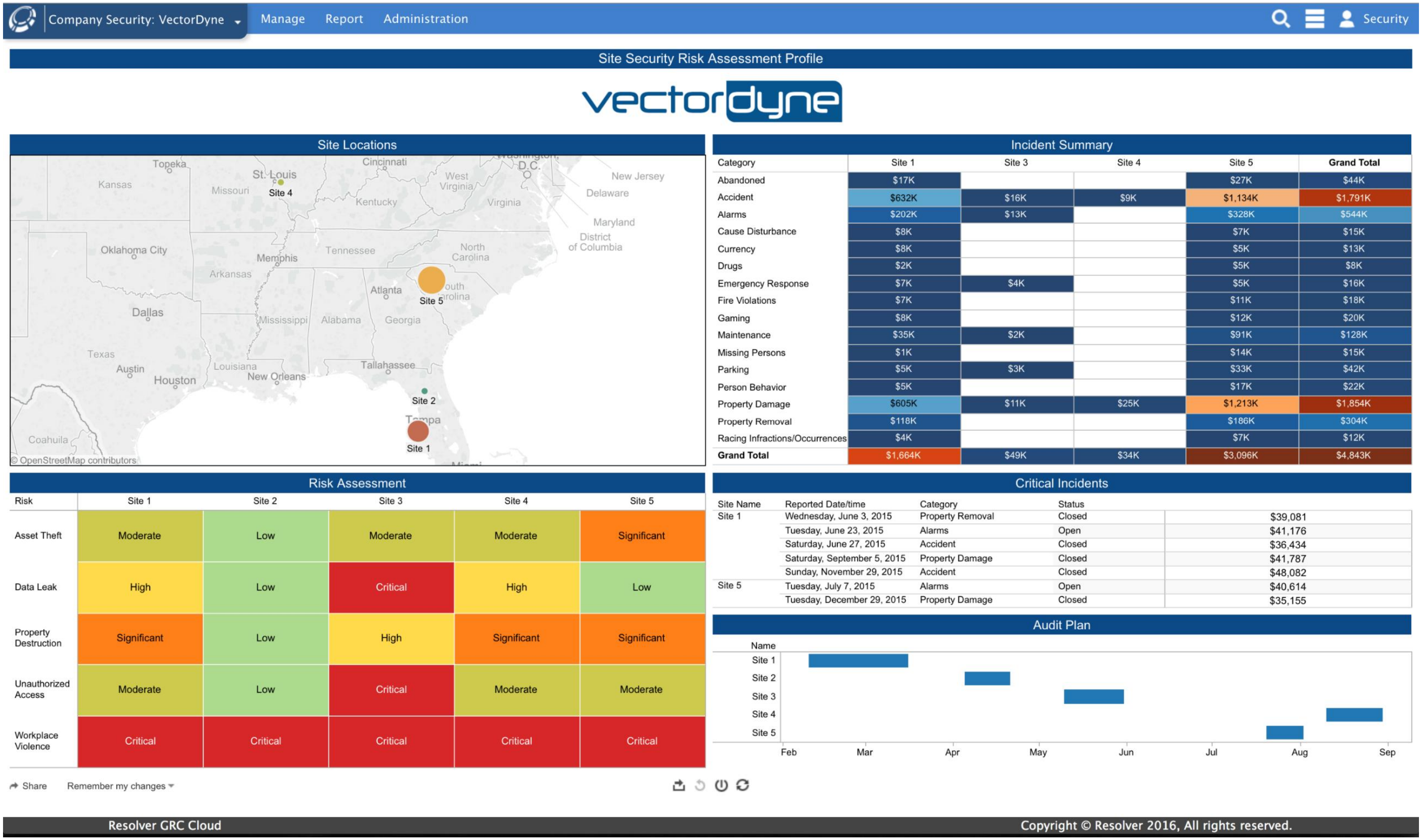
Business Intelligence

Link Analysis

AUTOMATED WORKFLOW

TYPICAL Security Management Process

COMPLETE Security Management Process



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

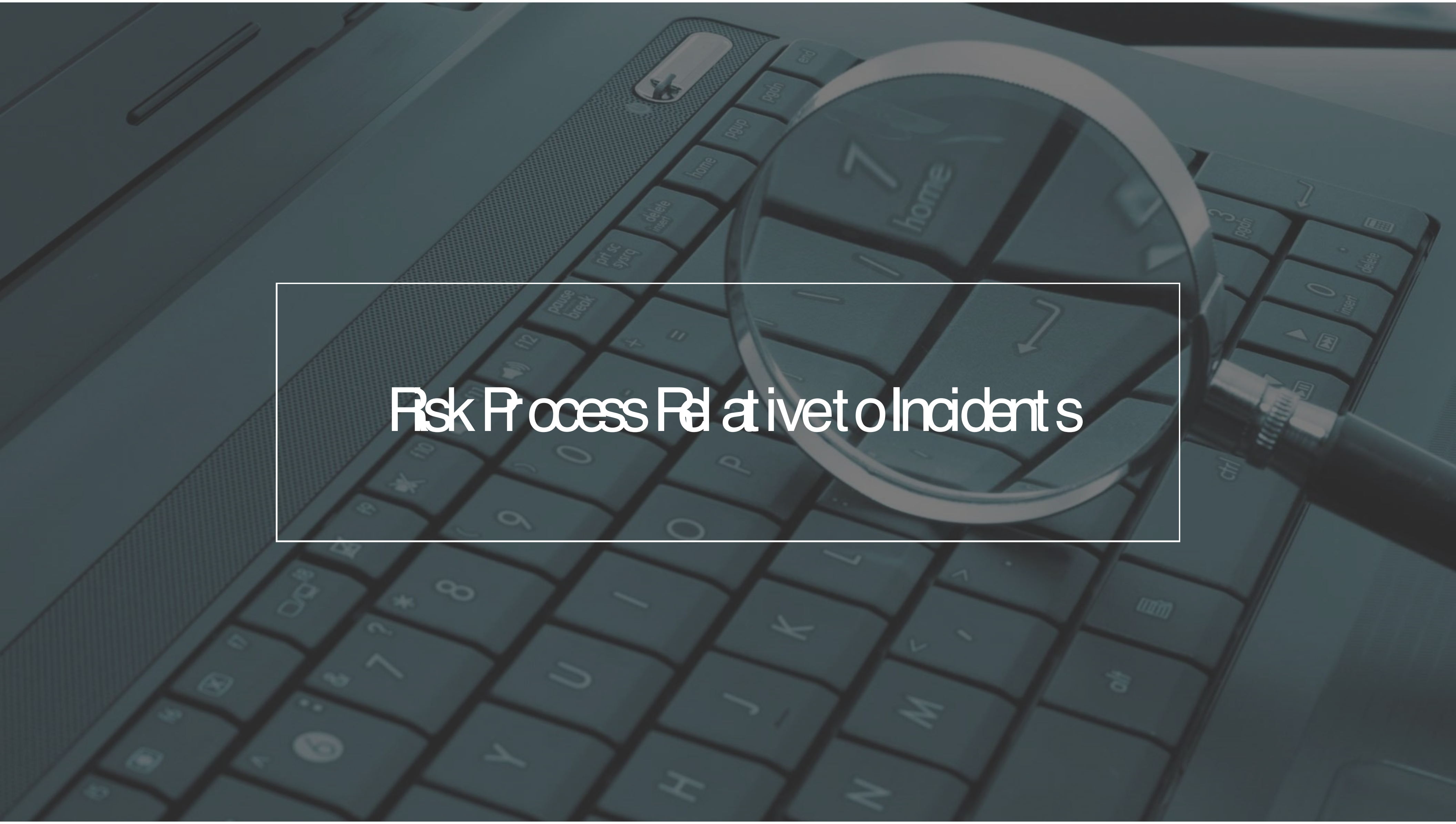
Critical Incidents

Site Name	Reported Date/time	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

Resolver GRC Cloud

:RESOLVER



Risk Process Relative to Incidents

EST. 2009

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.

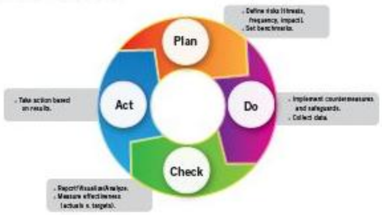
What is Incident Management?

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 1: Plan and Prepare

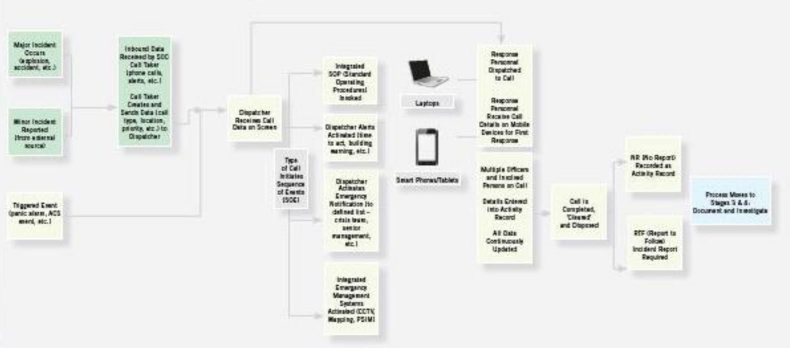
The Deming Cycle

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.



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

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)

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

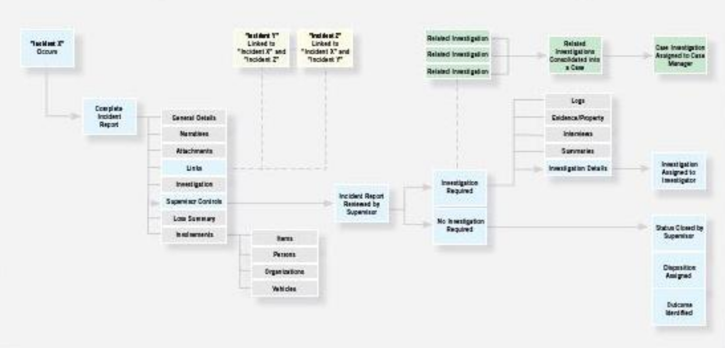
Call is Completed, 'Cleared' and Disposed

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



"Incident X" Occurs

Complete Incident Report

General Details
Narratives
Attachments
Links
Investigation
Supervisor Controls
Loss Summary
Involvements

Items
Persons
Organizations
Vehicles

"Incident Y" Linked to "Incident X" and "Incident Z"

"Incident Z" Linked to "Incident X" and "Incident Y"

Incident Report Reviewed by Supervisor

Investigation Required

No Investigation Required

Related Investigation
Related Investigation
Related Investigation

Related Investigations Consolidated into a Case

Case Investigation Assigned to Case Manager

Logs
Evidence/Property
Interviews
Summaries
Investigation Details

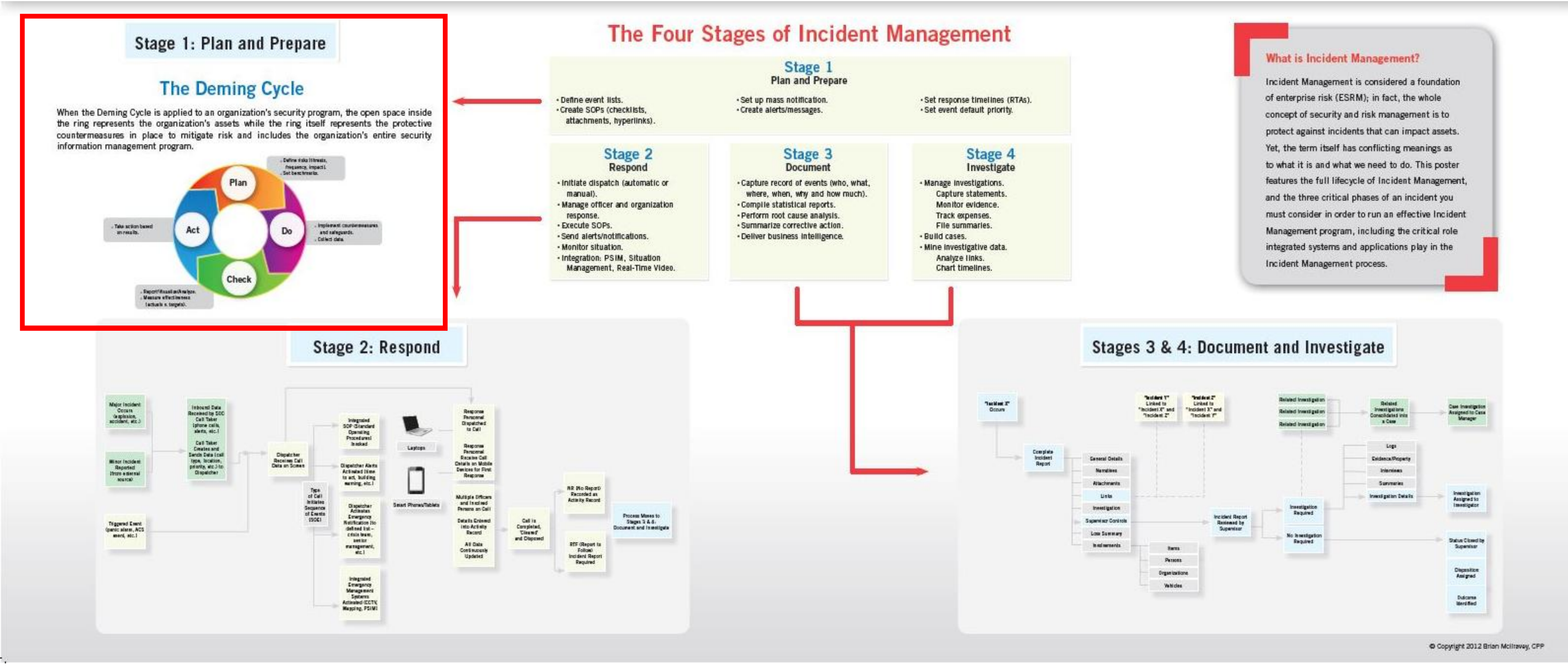
Investigation Assigned to Investigator

Status Closed by Supervisor

Disposition Assigned

Outcome Identified

:RESOLVER



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

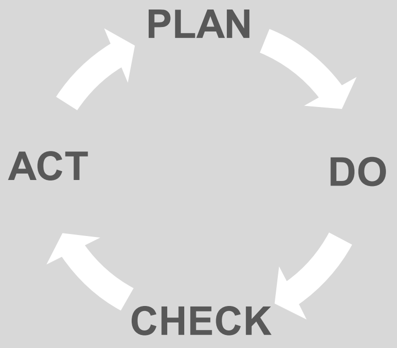
Major Incident Occurs (explosion, accident, etc.)
Minor Incident Reported (from external source)
Triggered Event (panic alarm, ACS event, etc.)
Inbound Data Received by SOC Call Taker (phone calls, alerts, etc.)
Call Taker Creates and Sends Data (call type, location, priority, etc.) to Dispatcher
Dispatcher 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

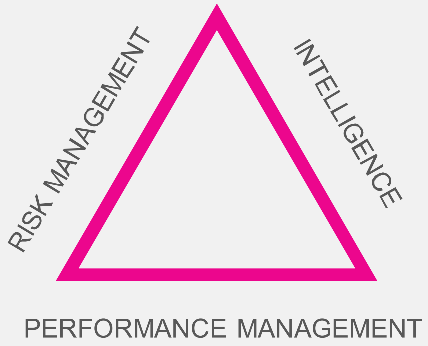
Angles of Incident Management

How does Incident Management fit into your risk management program?

THE DEMING CYCLE

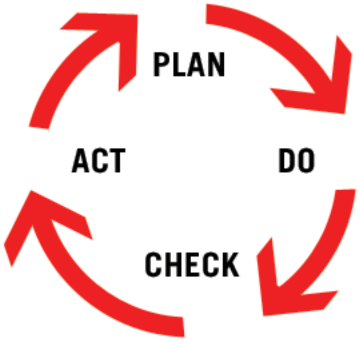


ANGLES OF INCIDENT MANAGEMENT



Risk Management

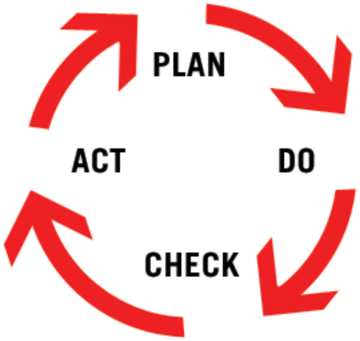
Define Risks (Threats, Frequency, Impact)



Risk Management

Define Risks (Threats, Frequency, Impact)

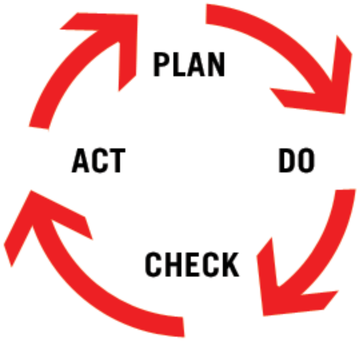
INTERNAL THEFT



Risk Management

Define Risks (Threats, Frequency, Impact)

INTERNAL THEFT

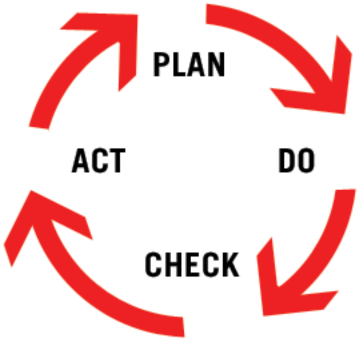


IMPLEMENT COUNTERMEASURES
& SAFEGUARDS

Risk Management

Define Risks (Threats, Frequency, Impact)

INTERNAL THEFT



IMPLEMENT COUNTERMEASURES & SAFEGUARDS

MEASURE EFFECTIVENESS

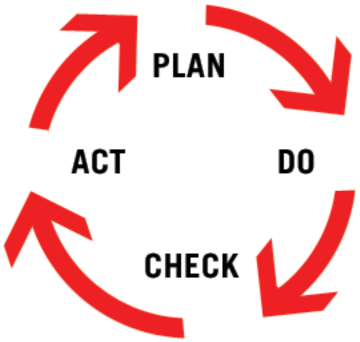
↓

Incident Management
+ or -

Risk Management

Define Risks (Threats, Frequency, Impact)

INTERNAL THEFT



TAKE ACTION BASED ON RESULTS

IMPLEMENT COUNTERMEASURES
& SAFEGUARDS

MEASURE EFFECTIVENESS

↓

Incident Management
+ or -

PDF-XChange Click to buy NOW! www.docu-track.com

Risk Management

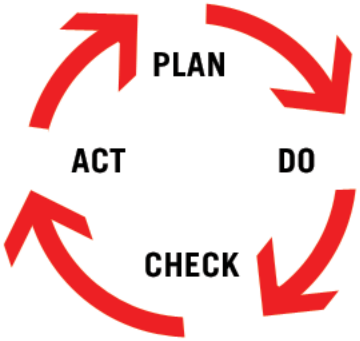
Risk Management

- Threat Frequency/Event History
- SLE
- ALE
- Freq Dist (heat mapping)

Define Risks (Threats, Frequency, Impact)

INTERNAL THEFT

TAKE ACTION BASED ON RESULTS



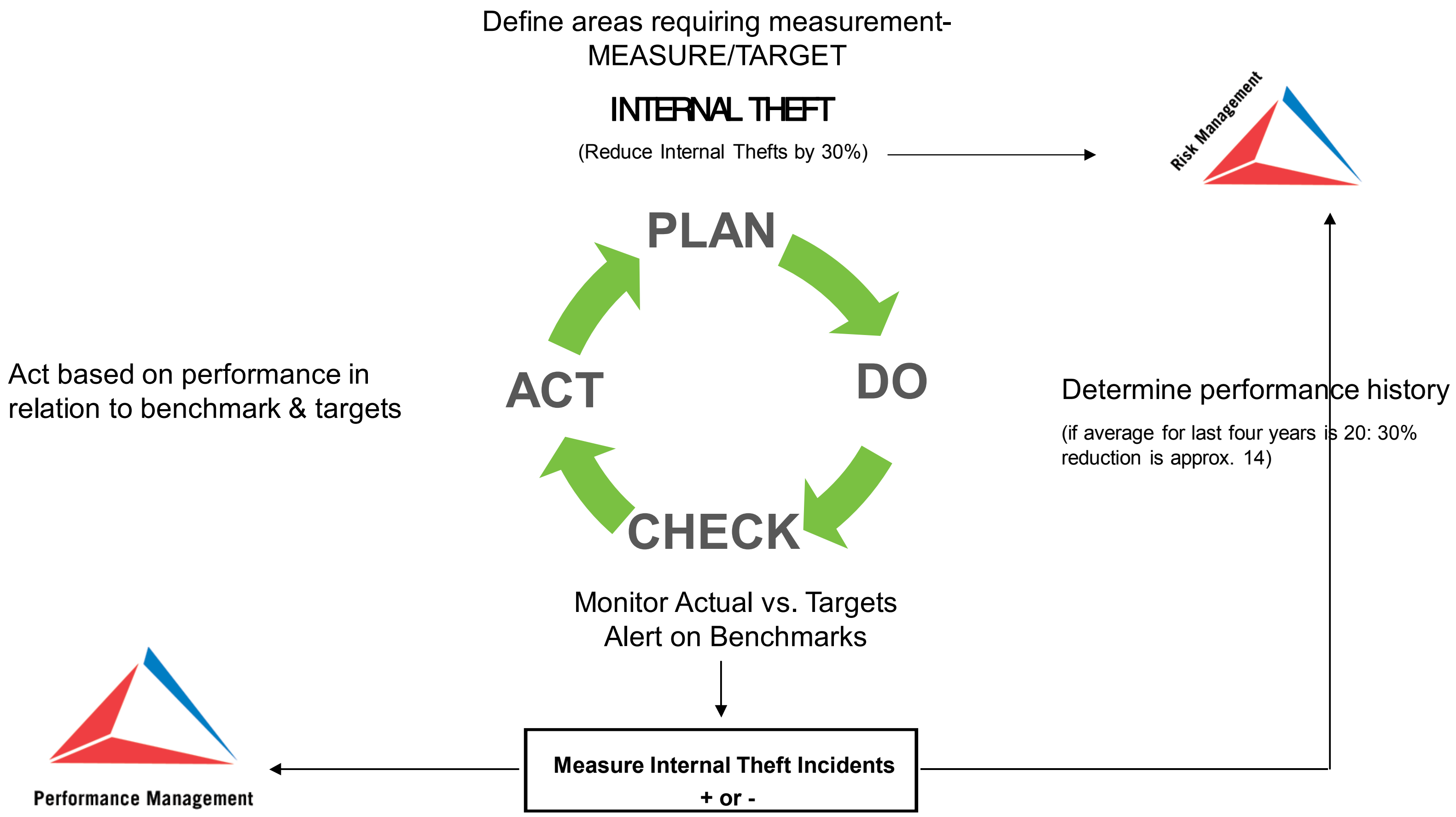
IMPLEMENT COUNTERMEASURES
& SAFEGUARDS

MEASURE EFFECTIVENESS

↓

Incident Management
+or -

Performance Measurement & Risk Management



Define areas requiring measurement-
MEASURE/TARGET

INTERNAL THEFT

(Reduce Internal Thefts by 30%)

Risk Management

PLAN

DO

CHECK

ACT

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 Vulnerabilities x Impact

Risks = Threats x Frequency x Impact

Risks = Threats x Vulnerabilities x Impact

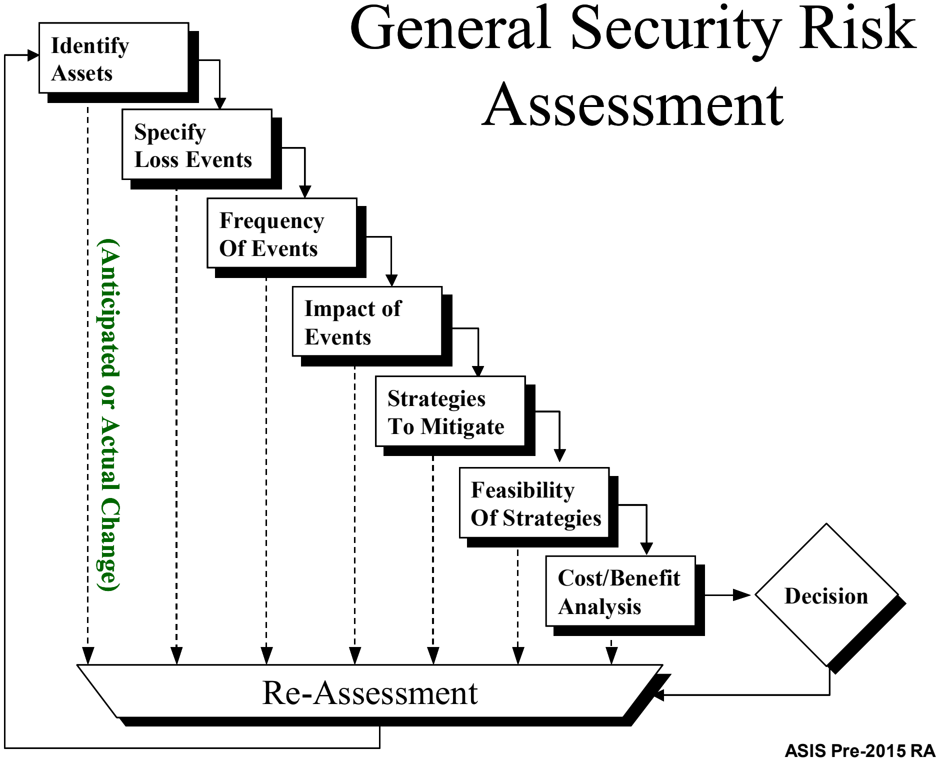
Risks = Threats x Frequency x Impact

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

Risks = Threats x Vulnerabilities x Impact

Risks = Threats x Frequency x Impact

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



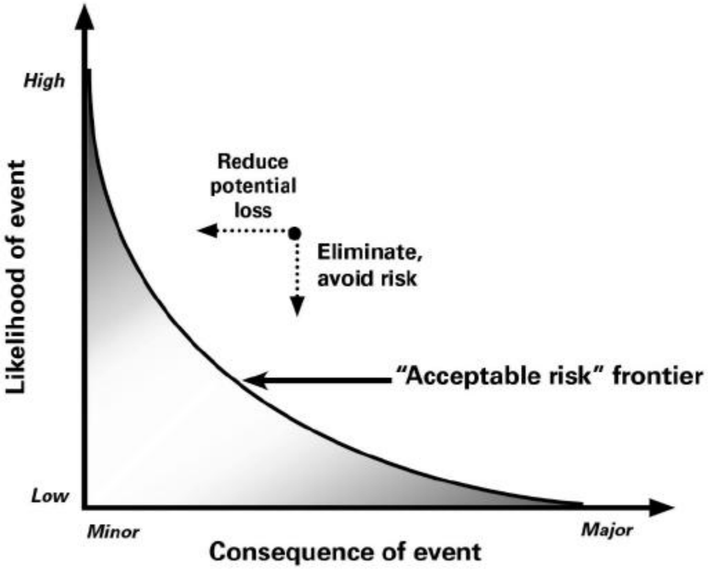
General Security Risk Assessment

ASIS Pre-2015 RA Model

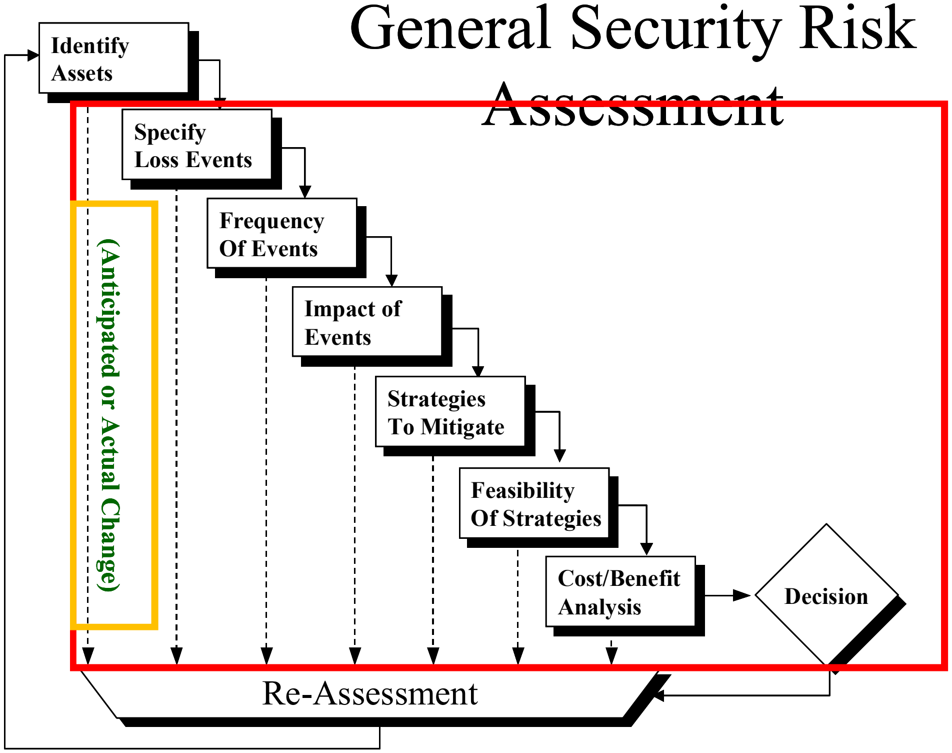
Risks = Threats x Vulnerabilities x Impact

Risks = Threats x Frequency x Impact

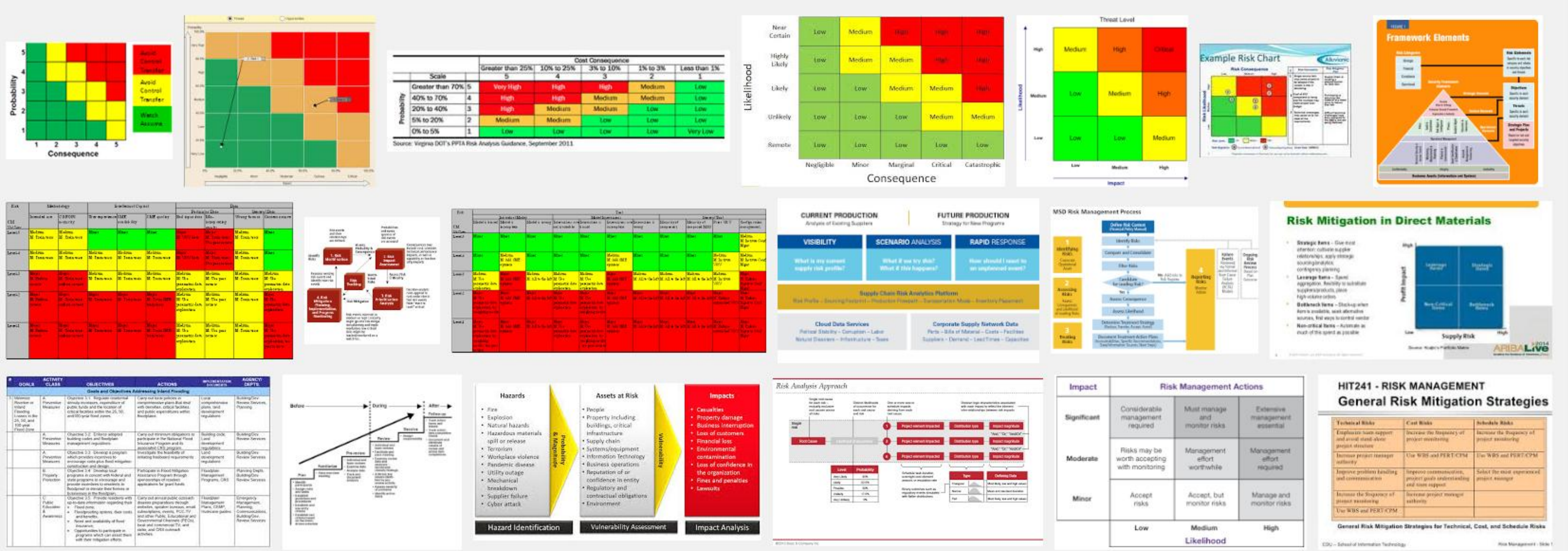
PA x (1-SE) x C$ = R$ + SE$



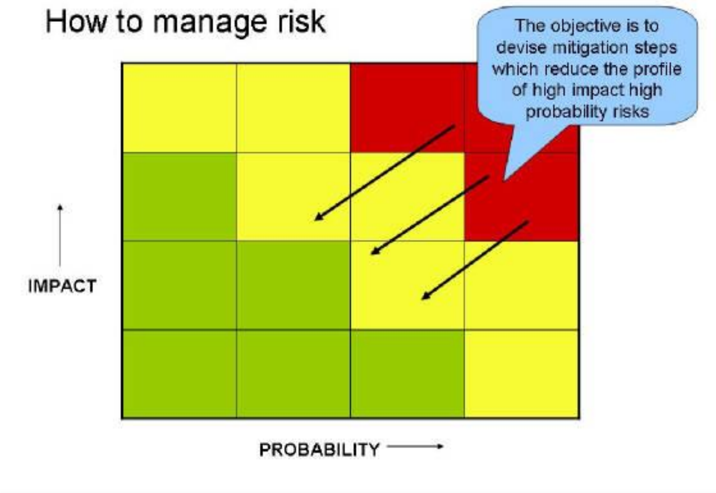
General Security Risk Assessment

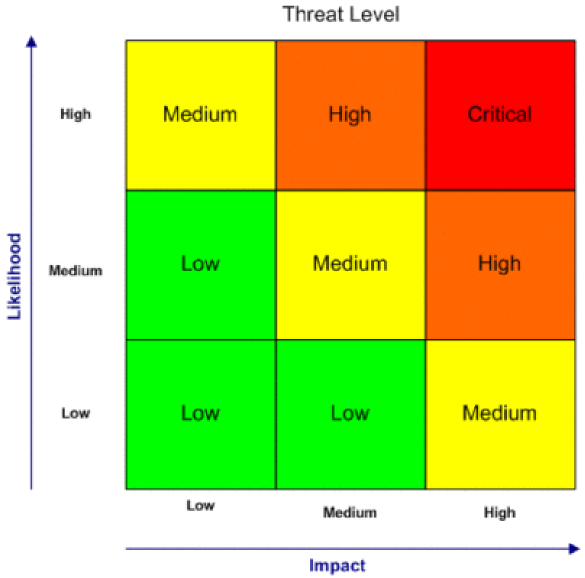


WE ALSO SEE RISK BY COLOR

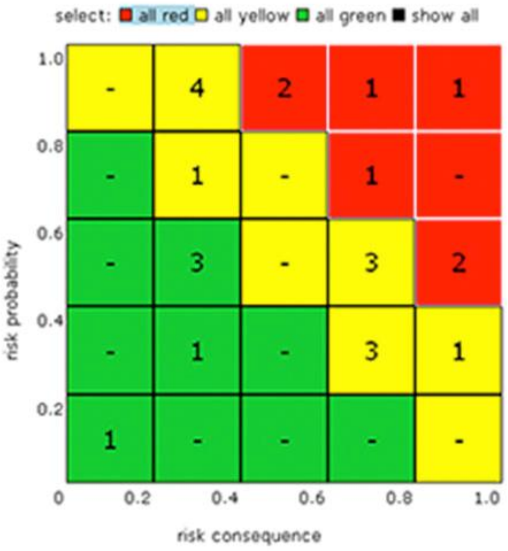


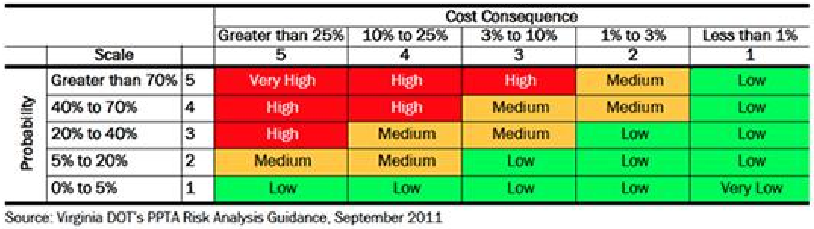
WE ALSO SEE RISK BY COLOR


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



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





			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

2015-2016 ASISANSI Risk Assessment Model

2015-2016 ASIS ANSI Risk Assessment Model

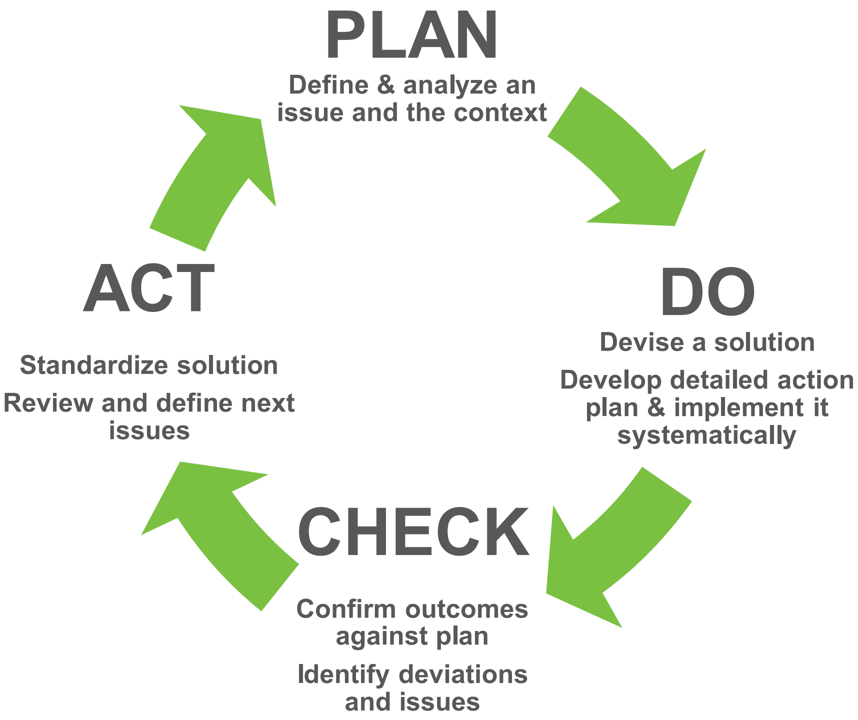
The PDCA model is a clear, systematic and documented approach to:

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;



PLAN

Define & analyze an issue and the context

DO

Devise a solution

Develop detailed action plan & implement it systematically

CHECK

Confirm outcomes against plan

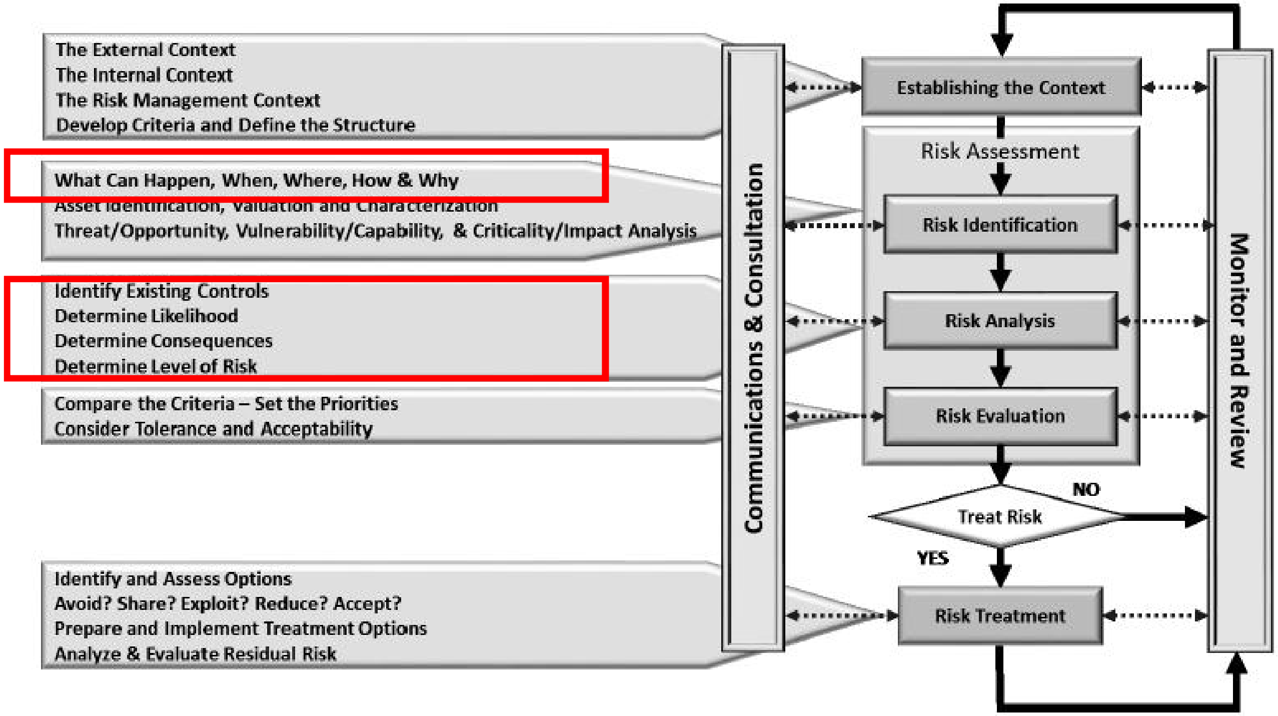
Identify deviations and issues

ACT

Standardize solution

Review and define next issues

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

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

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

How and Why

How and Why

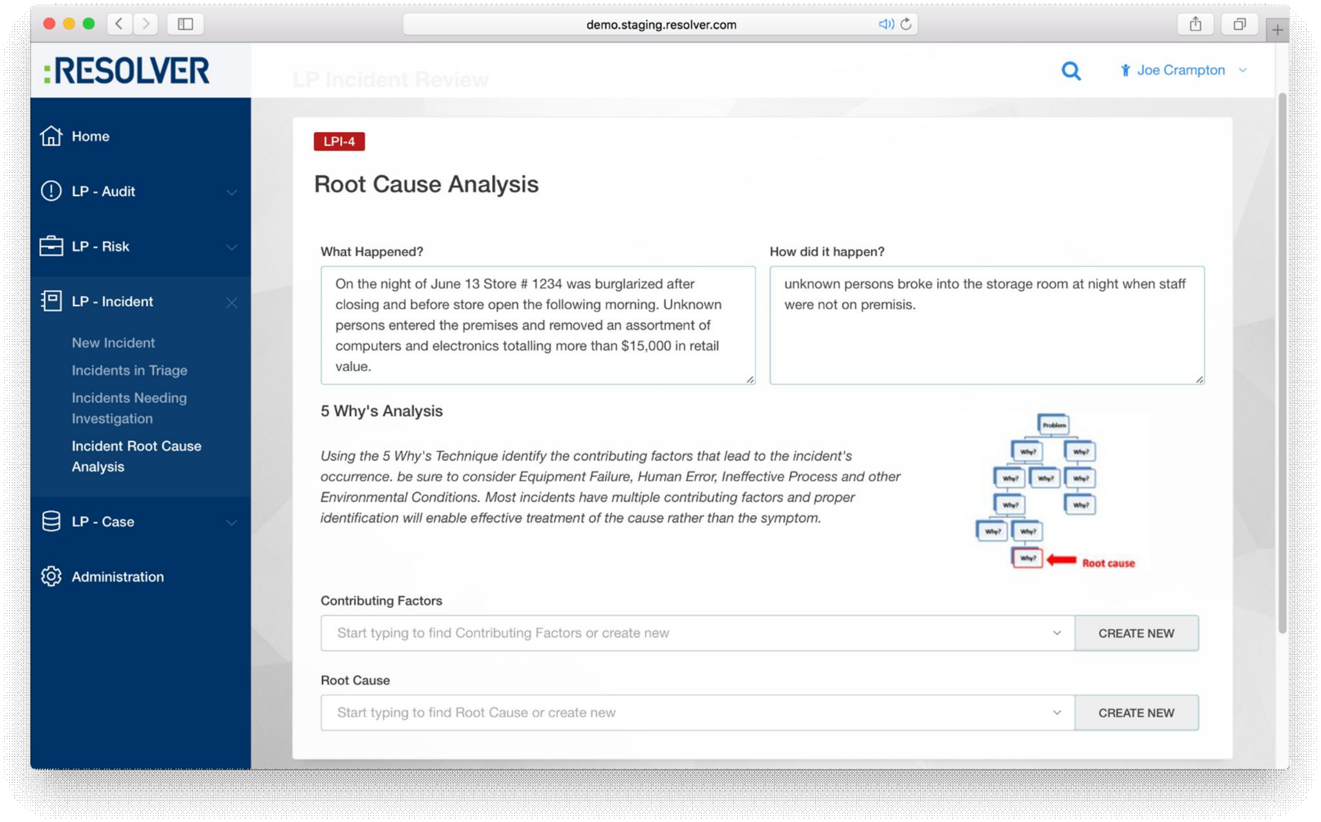
Cause

Mechanism

Manner

How and Why

Cause Mechanism Manner



Root Cause Analysis

What Happened?

On the night of June 13 Store # 1234 was burglarized after closing and before store open the following morning. Unknown persons entered the premises and removed an assortment of computers and electronics totalling more than $15,000 in retail value.

How did it happen?

unknown persons broke into the storage room at night when staff were not on premisis.

5 Why's Analysis

Using the 5 Why's Technique identify the contributing factors that lead to the incident's occurrence. be sure to consider Equipment Failure, Human Error, Ineffective Process and other Environmental Conditions. Most incidents have multiple contributing factors and proper identification will enable effective treatment of the cause rather than the symptom.

Contributing Factors

Start typing to find Contributing Factors or create new

Root Cause

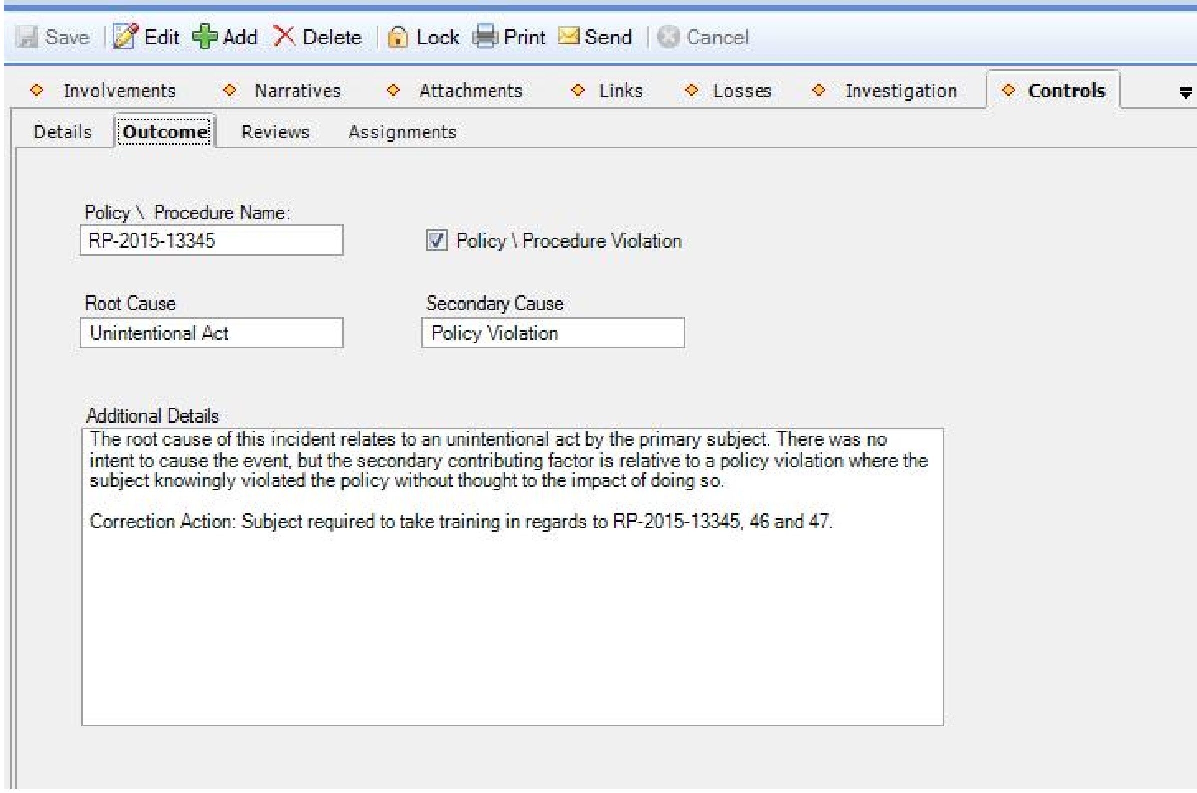
Start typing to find Root Cause or create new

How and Why

Cause

Mechanism

Manner



Policy \ Procedure Name: RP-2015-13345

☑ Policy \ Procedure Violation

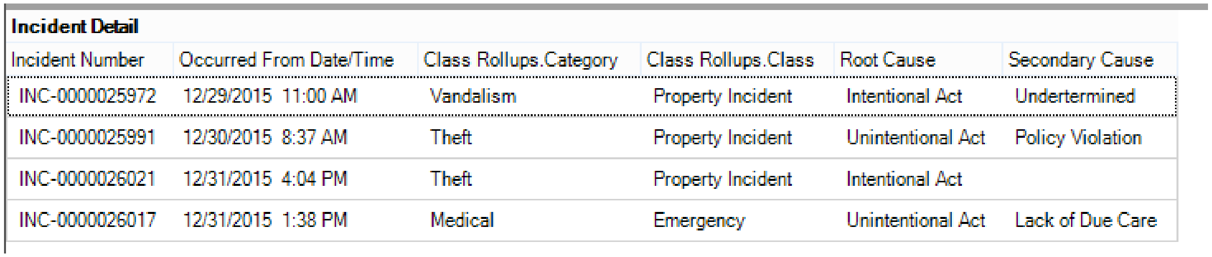
Root Cause: Unintentional Act

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.

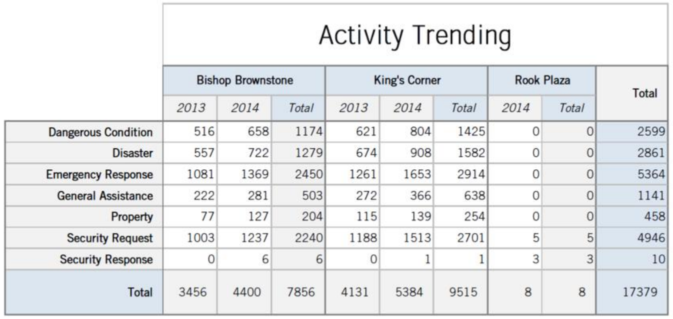
Correction Action: Subject required to take training in regards to RP-2015-13345, 46 and 47.



Incident Detail

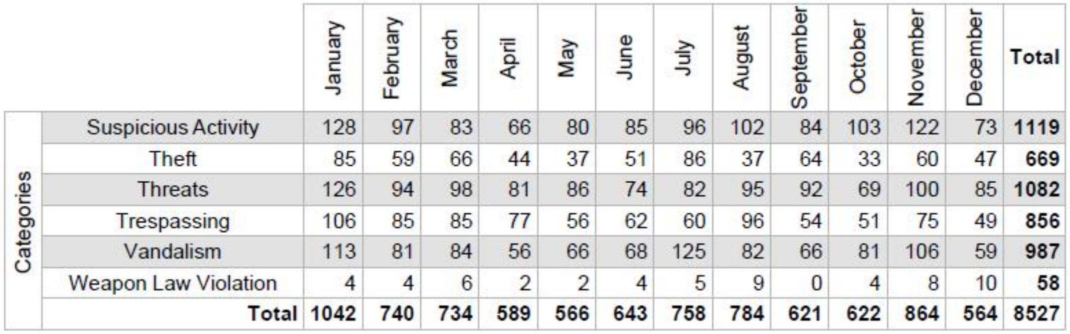
Incident Number	Occurred From Date/Time	Class Rollups.Category	Class Rollups.Class	Root Cause	Secondary Cause
INC-0000025972	12/29/2015 11:00 AM	Vandalism	Property Incident	Intentional Act	Undertermined
INC-0000025991	12/30/2015 8:37 AM	Theft	Property Incident	Unintentional Act	Policy Violation
INC-0000026021	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

What , Where, When
AKA FD, TF, ALE, SLE

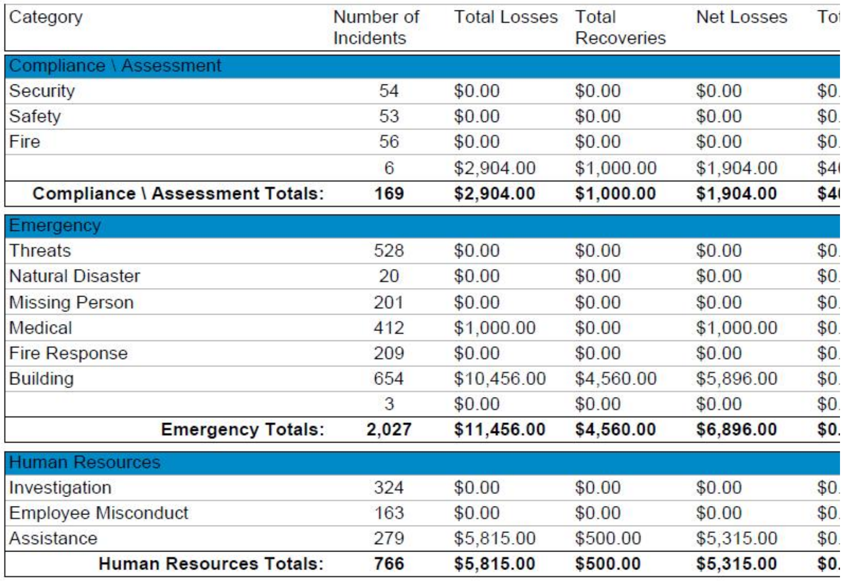


Activity Trending

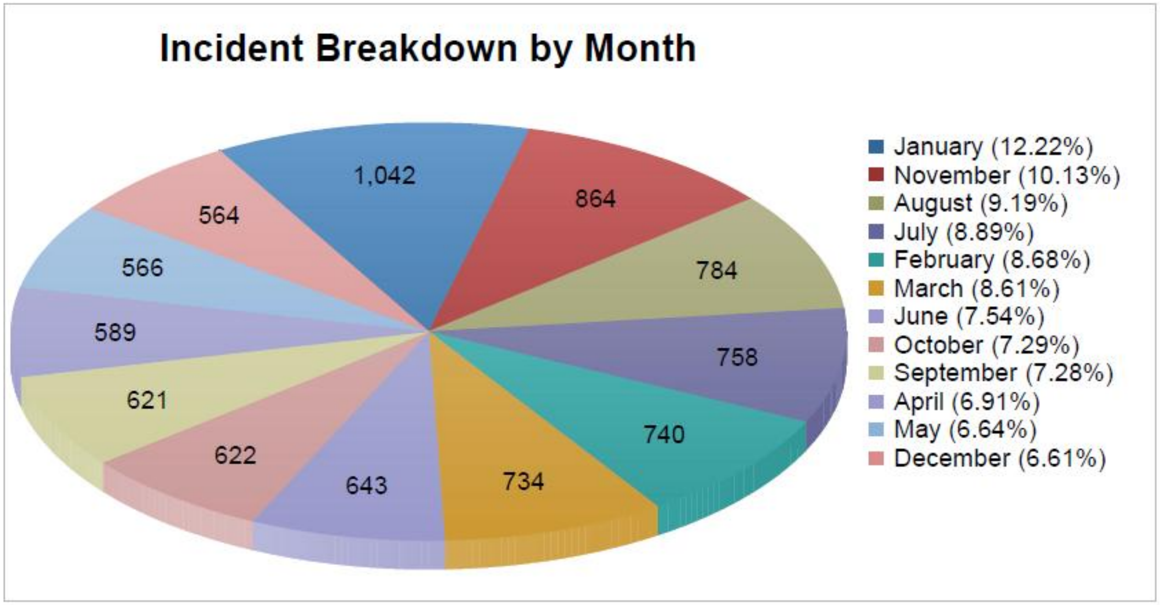
	Bishop Brownstone			King's Corner			Rook Plaza		Total
	2013	*2014*	*Total*	*2013*	*2014*	*Total*	*2014*	*Total*	
Dangerous Condition	516	658	1174	621	804	1425	0	0	2599
Disaster	557	722	1279	674	908	1582	0	0	2861
Emergency Response	1081	1369	2450	1261	1653	2914	0	0	5364
General Assistance	222	281	503	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



Categories		January	February	March	April	May	June	July	August	September	October	November	December	Total
	Suspicious Activity	128	97	83	66	80	85	96	102	84	103	122	73	**1119**
	Theft	85	59	66	44	37	51	86	37	64	33	60	47	**669**
	Threats	126	94	98	81	86	74	82	95	92	69	100	85	**1082**
	Trespassing	106	85	85	77	56	62	60	96	54	51	75	49	**856**
	Vandalism	113	81	84	56	66	68	125	82	66	81	106	59	**987**
	Weapon Law Violation	4	4	6	2	2	4	5	9	0	4	8	10	**58**
	Total	**1042**	**740**	**734**	**589**	**566**	**643**	**758**	**784**	**621**	**622**	**864**	**564**	**8527**

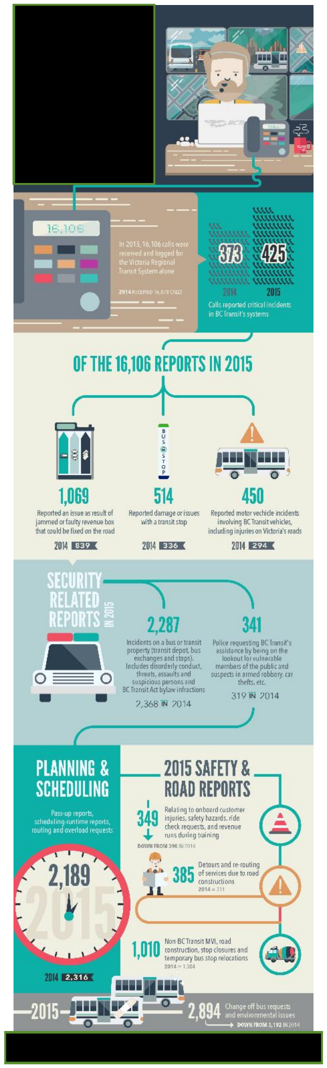


Category	Number of Incidents	Total Losses	Total Recoveries	Net Losses	To
Compliance \ Assessment					
Security	54	$0.00	$0.00	$0.00	$0.
Safety	53	$0.00	$0.00	$0.00	$0.
Fire	56	$0.00	$0.00	$0.00	$0.
	6	$2,904.00	$1,000.00	$1,904.00	$4
Compliance \ Assessment Totals:	**169**	**$2,904.00**	**$1,000.00**	**$1,904.00**	**$4**
Emergency					
Threats	528	$0.00	$0.00	$0.00	$0.
Natural Disaster	20	$0.00	$0.00	$0.00	$0.
Missing Person	201	$0.00	$0.00	$0.00	$0.
Medical	412	$1,000.00	$0.00	$1,000.00	$0.
Fire Response	209	$0.00	$0.00	$0.00	$0.
Building	654	$10,456.00	$4,560.00	$5,896.00	$0.
	3	$0.00	$0.00	$0.00	$0.
Emergency Totals:	**2,027**	**$11,456.00**	**$4,560.00**	**$6,896.00**	**$0.**
Human Resources					
Investigation	324	$0.00	$0.00	$0.00	$0.
Employee Misconduct	163	$0.00	$0.00	$0.00	$0.
Assistance	279	$5,815.00	$500.00	$5,315.00	$0.
Human Resources Totals:	**766**	**$5,815.00**	**$500.00**	**$5,315.00**	**$0.**



Incident Breakdown by Month

[redacted]



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

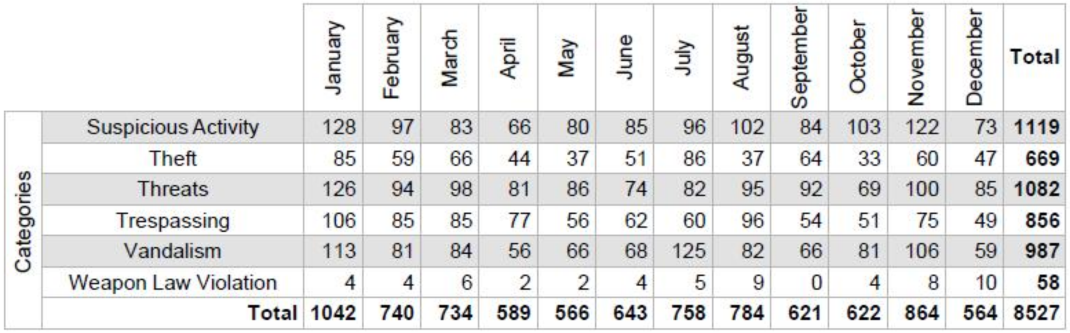
349
Relating to onboard customer injuries, safety hazards, ride check requests, and revenue runs during training
DOWN FROM 390 IN 2014

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

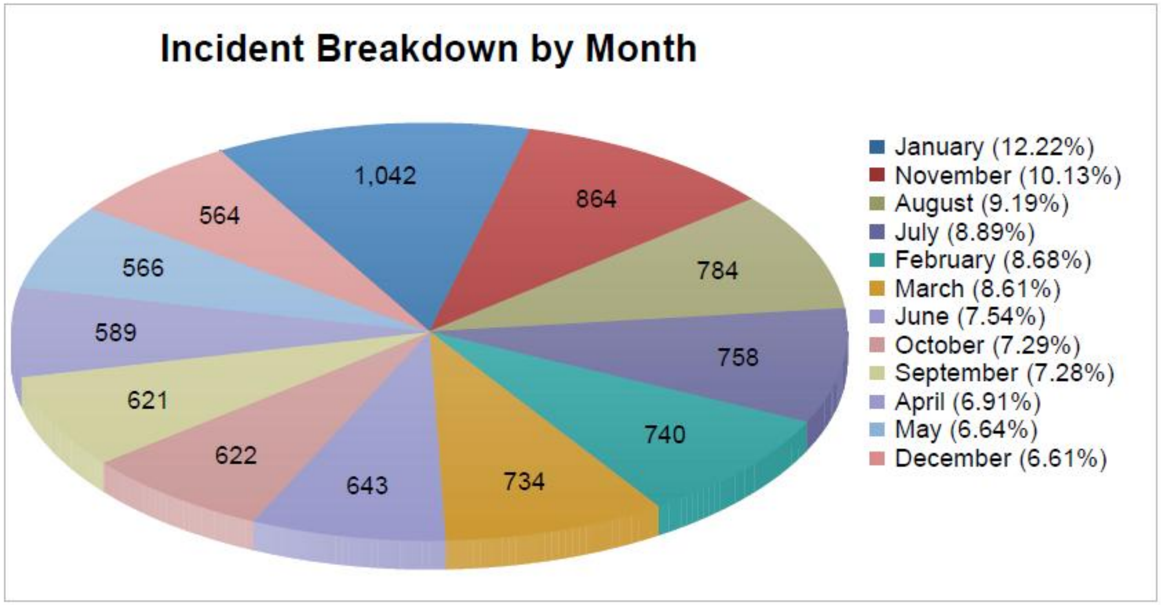
1,010
Non-BC Transit MVI, road construction, stop closures and temporary bus stop relocations
2014 = 1,004

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

[redacted]



Categories	January	February	March	April	May	June	July	August	September	October	November	December	Total
Suspicious Activity	128	97	83	66	80	85	96	102	84	103	122	73	**1119**
Theft	85	59	66	44	37	51	86	37	64	33	60	47	**669**
Threats	126	94	98	81	86	74	82	95	92	69	100	85	**1082**
Trespassing	106	85	85	77	56	62	60	96	54	51	75	49	**856**
Vandalism	113	81	84	56	66	68	125	82	66	81	106	59	**987**
Weapon Law Violation	4	4	6	2	2	4	5	9	0	4	8	10	**58**
Total	**1042**	**740**	**734**	**589**	**566**	**643**	**758**	**784**	**621**	**622**	**864**	**564**	**8527**



Incident Breakdown by Month

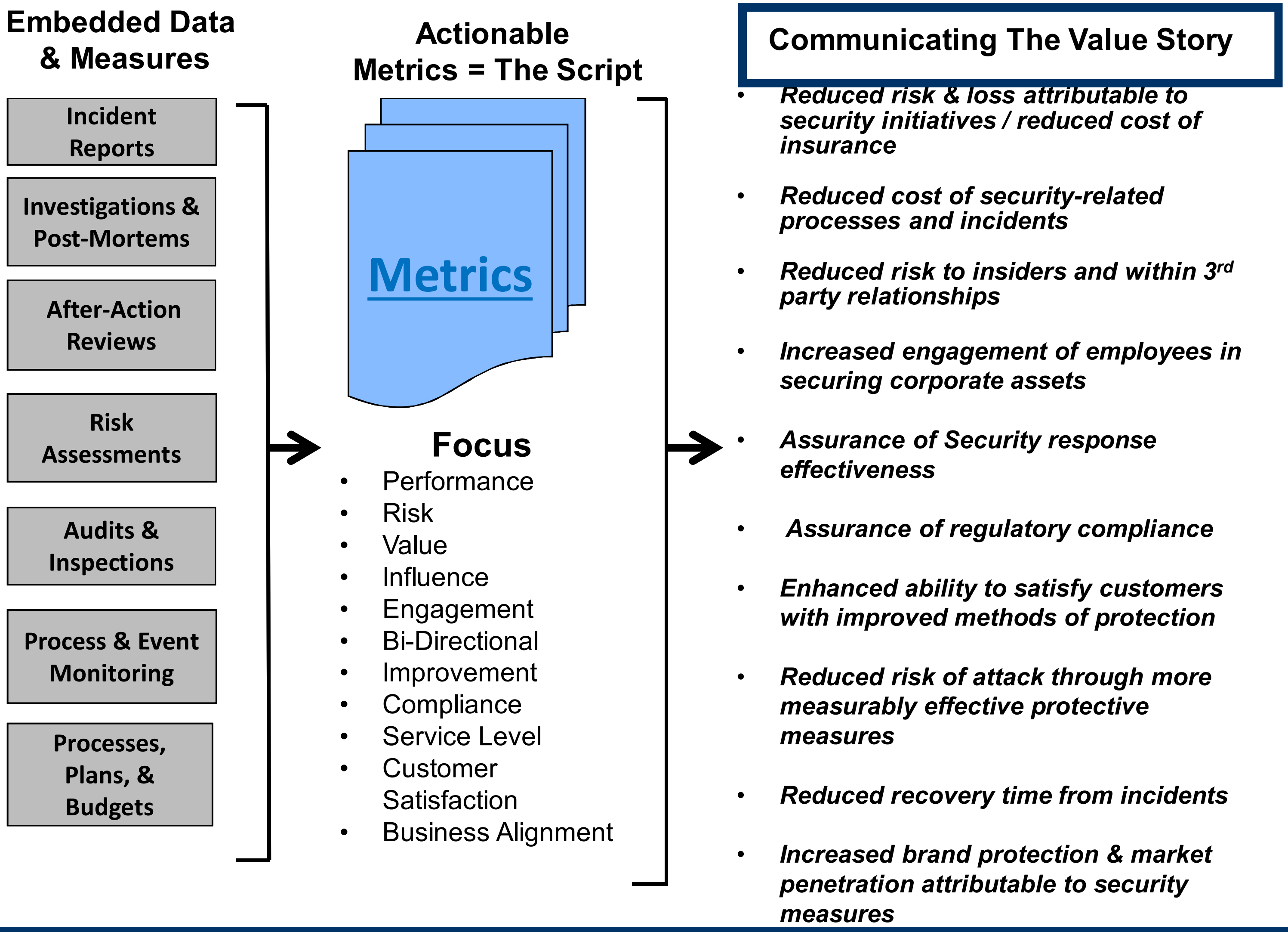
“

Hook into the bigger aggregators”

“..Incident management tools have helped him to manage physical and information security incidents but 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 & performance...”

– Enterprise Security Risk Management: How Great Risks Lead to Great Deeds
A Benchmarking Survey and White Paper



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

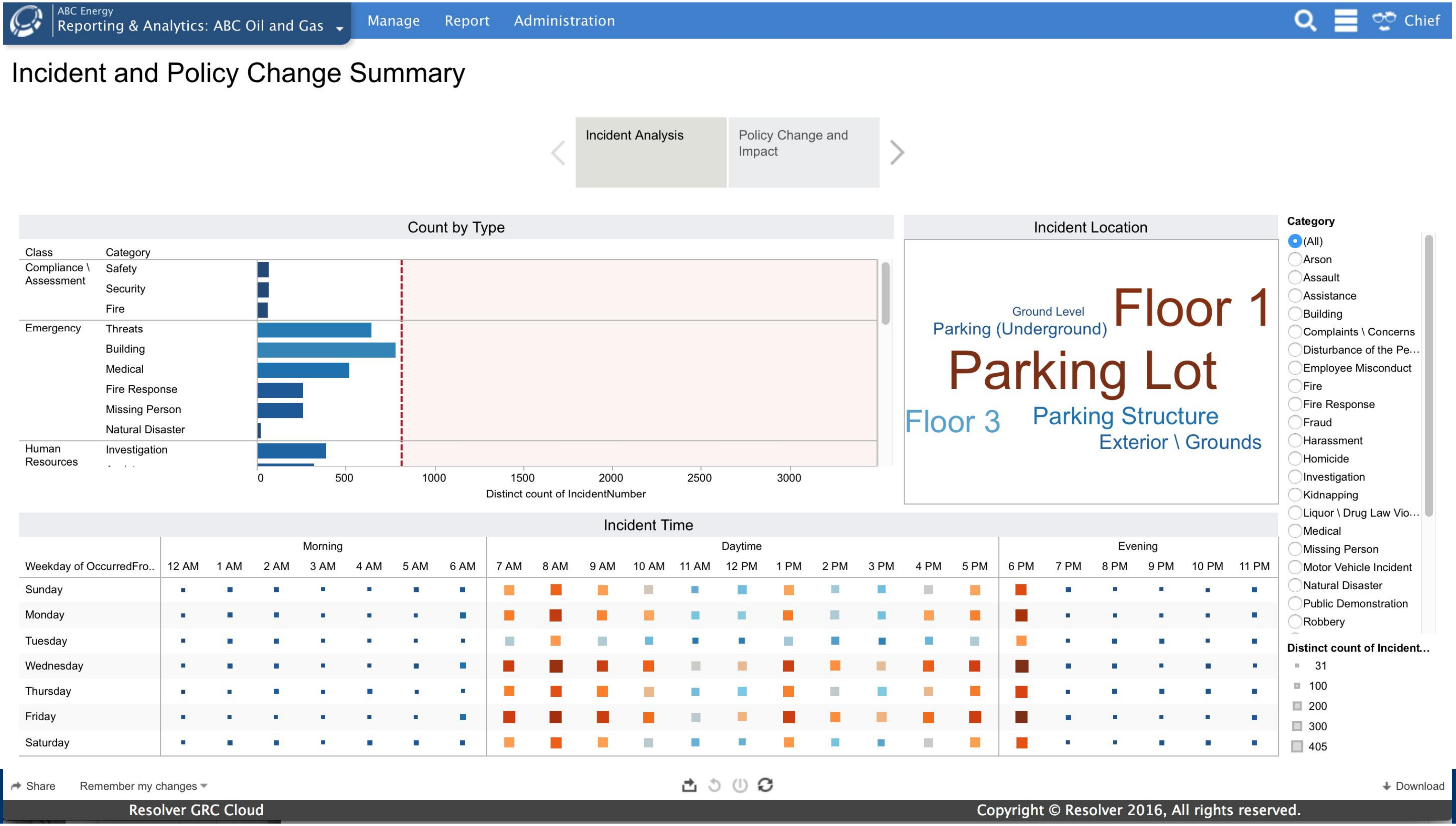
Metrics

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*



Incident and Policy Change Summary

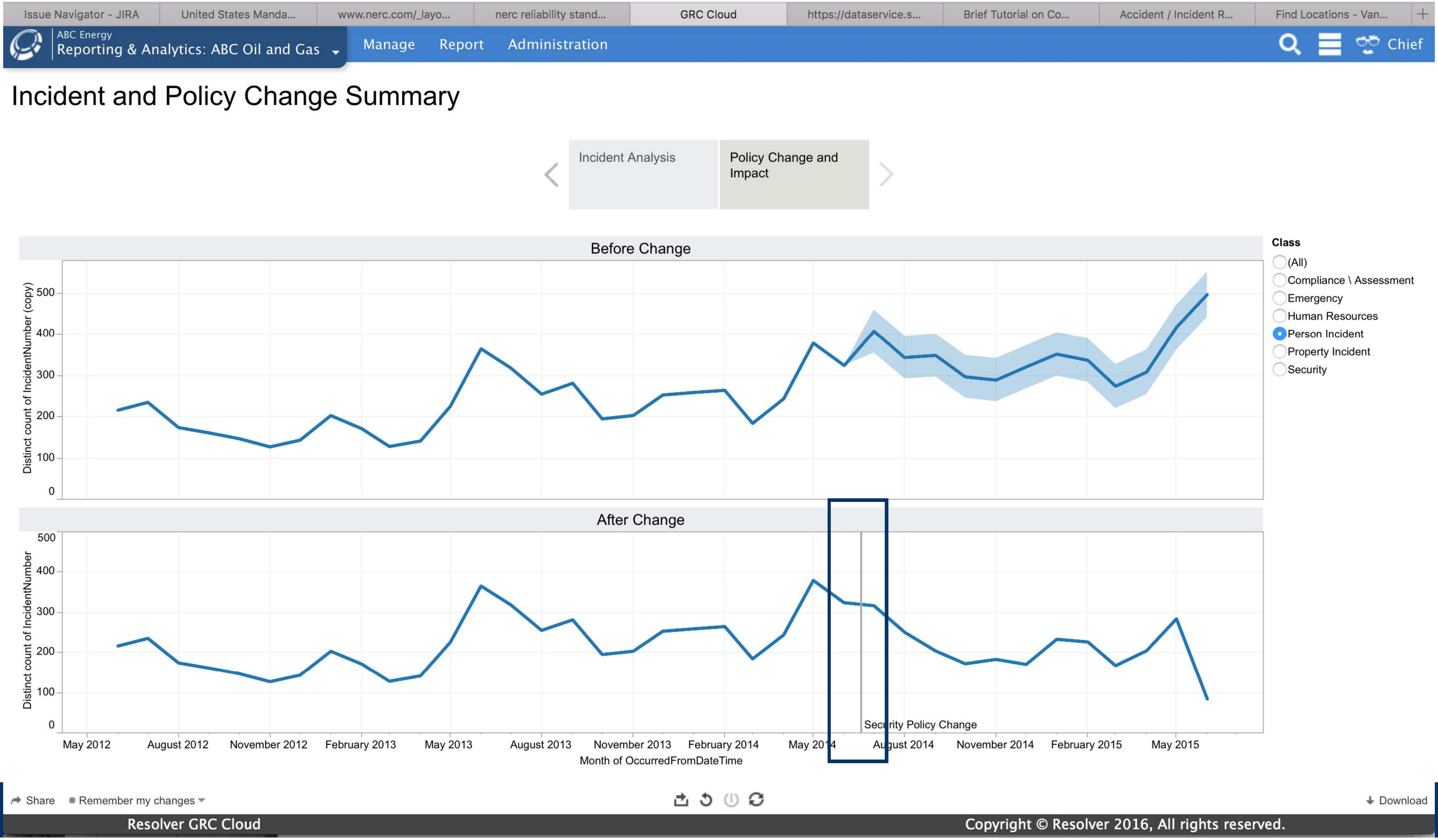
Category

● (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

Distinct count of Incident…

▪ 31
▪ 100
□ 200
□ 300
□ 405

Resolver GRC Cloud



Incident and Policy Change Summary

Class

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

Obsessing Over Raw Numbers

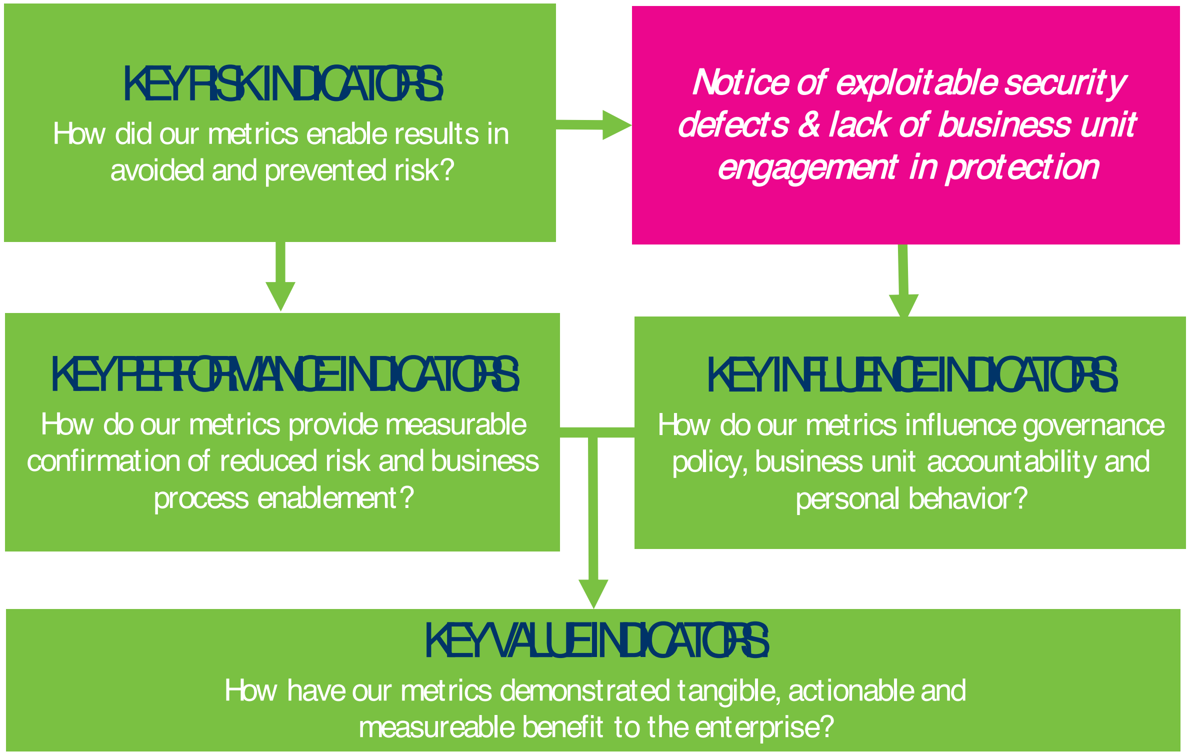
"One of the hurdles we face in the security industry is that while the processes and systems used to collect and manage data have improved tremendously, there has been comparatively little attention given to the analysis and effective communication of that data.

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)"

Risk Indicators

George campbell,
security executive council



KEY RISK INDICATORS
How did 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 measureable benefit to the enterprise?

customer
research
organization
performance
complex
probability
retention
assessment
data
identification
management
process
risk
sales
customer
plan
management
analysis
planning
implementation
monitor
risk
performance
retention
impact
organization
management
retention
performance
opportunity
project
assessment
cost
management
treatment
project
plan
strategy
research
resources
important
organization
risk
performance
evaluation

retention
customer
research
complex
probability
data
assessment
identification
process
risk
sales
customer
plan
analysis
planning
implementation
monitor
risk
retention
impact
opportunity
management
project
risk
strategy
assessment
performance
cost
evaluation
data
sales
organization
process
management
performance
cost
research
Performance
Management
data
management
treatment
retention
impact
project
plan
strategy
data
research
management
resources
risk
performance
assessment
context
performance
important
evaluation
performance
organization
data
scope
project

RISK & INCIDENTS: SAME SAND – Different CASTLES

"That's all Folks!"

Q and A Time

:RESOLVER

RISK-incidents:
same playground, different castles

Canadian Security
THE PUBLICATION FOR PROFESSIONAL SECURITY MANAGEMENT