Internal Risk Controls
An Organizational Approach

Earl Shockley – Vice President, Risk Management and Risk Controls

NRWG Meeting in Austin Texas, Dec 3, 2015

GridSME
SUBJECT MATTER EXPERTS

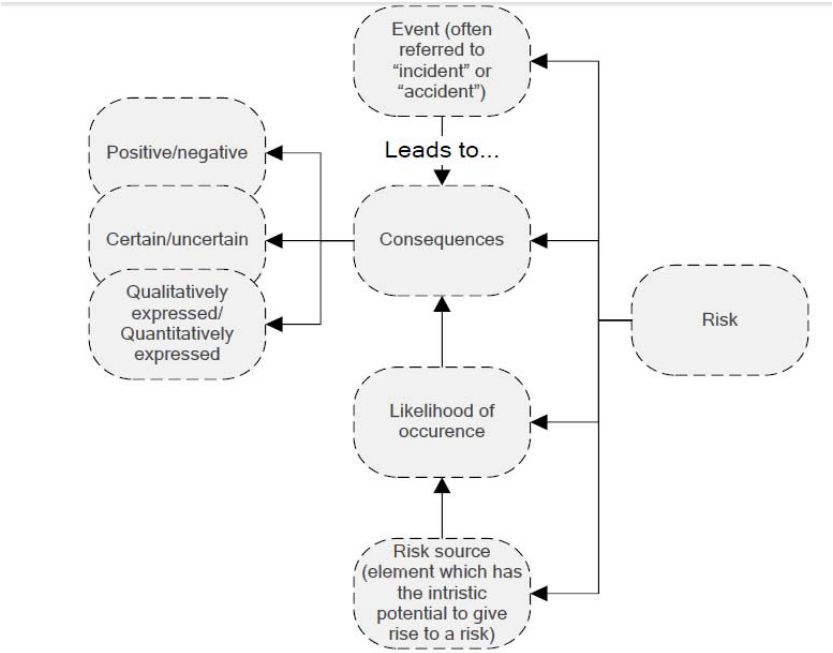
Agenda

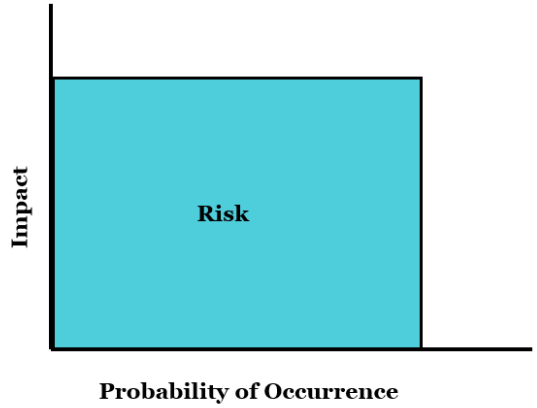
- Risk and Controls defined
- Why Internal Risk Controls are important
- Internal Risk Control System Frameworks
- What to Expect from Regulators
- Tools that can help

What is Risk?

"Risk"

What keeps you up at night, and, what you don't know about, that would keep you up at night.





Impact = (type & extent of damage)
Probability of Occurrence = (threat, vulnerability)

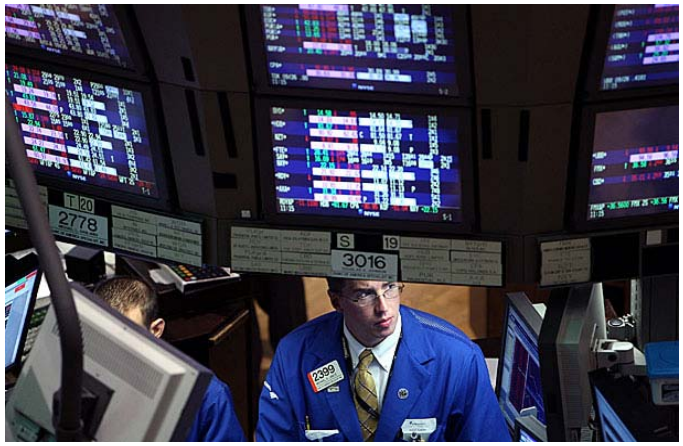
Internal Risk Controls Defined

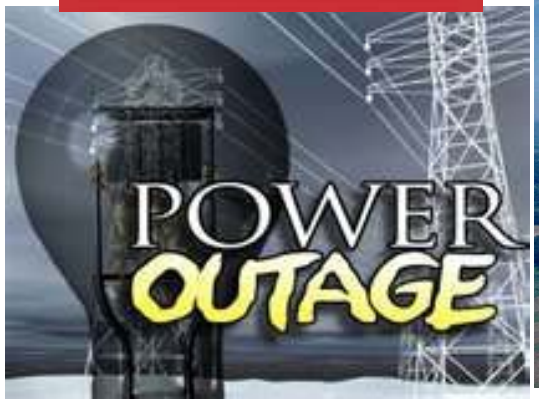
- Internal Controls are operating practices or activities that are established to provide reasonable assurance that specific objectives will be achieved.

- Primary objectives of an internal control system are:
  - Increased Reliability
  - Compliance with applicable policies, procedures, and regulations
  - Reliability and integrity of critical information;
  - Economic and efficient use of resources; and
  - Safeguarding of assets.

- Internal risk controls are the presence of control elements around your systems, processes and people that render organizational objectives free from unacceptable harm from risk and uncertainty.

Its Not Just About Compliance



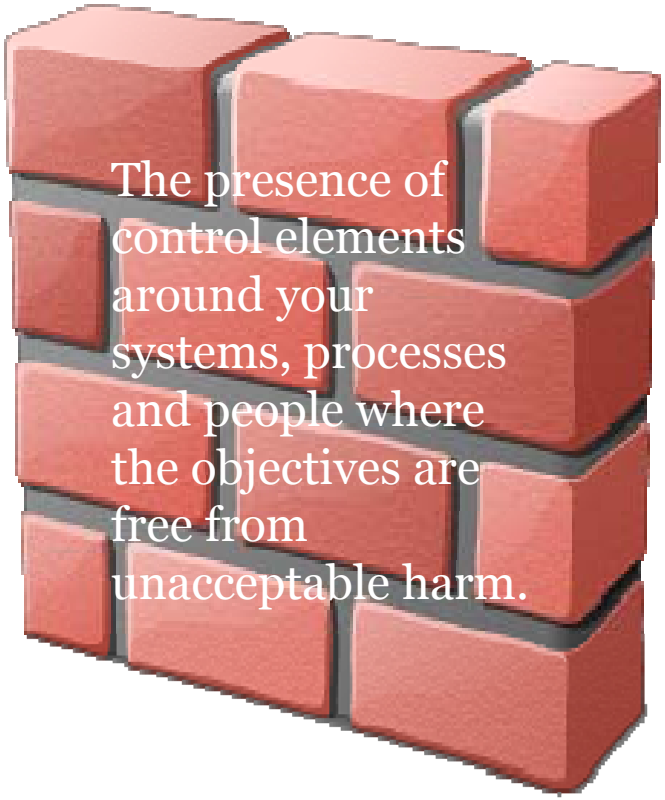


Events are not typically the outcome of one person's actions. More commonly, it is the result of a combination of faults in management and organizational activities.

Turner & Pidgeon - Man Made Disasters

Why Risk Controls are Important

Risk Controls prevent threats from reaching the targets



The presence of control elements around your systems, processes and people where the objectives are free from unacceptable harm.

Examples from the News

WASHINGTON AND THE WORLD

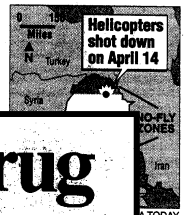
Report lays 'friendly fire' blame

Multiple errors in chopper downings

By Steve Komarow
USA TODAY

The "friendly fire" shooting down of U.S. helicopters over

firmed suspicions that were voiced soon after the incident: that the F-15 pilots mistook the Black Hawks for Iraqi Hind helicopters.



ing both sets of aircraft.

AWACS controllers failed to talk among themselves. If they had, the F-15s would have been warned they were targetting U.S. helicopters.

"This incident clearly shows us that technology, no matter how advanced, can't solve all of our problems," says Robert Gaskin, a former Air Force pilot, now vice president of Business Executives for National Security. "Ultimately, it comes down to human beings having to make crucial decisions."

Perry has promised repeatedly to lower the chances of such accidents.

Immediately after the tragedy, he ordered an end to "hair-trigger" firing at targets in the no-fly zone. That type of firing contributed to the accident. He has promised additional "corrective action."

Joining Perry will be Gen. John Shalikashvili, the chairman of the Joint Chiefs of Staff who once headed the Iraq operation, and Maj. Gen. James Andrus, the chief investigator.

Still under debate: whether to release TV cockpit tapes of the helicopter downings.

Apparently, Perry won't announce what punishment will be meted out to those responsible. Under military procedures, once the accident report is accepted, commanding officers use that as a basis for punishment, which could range from none to a court-martial.

Hospitals' drug errors cost lives, drain resources

By Tim Friend
USA TODAY

22 Jan 97

Prescription drug errors double a person's risk of dying in the hospital and cost an estimated $2 billion a year, new studies show.

Prescribing errors have become such a serious problem that hospitals should invest in ways to prevent them, the researchers say.

The studies in today's *Journal of the American Medical Association* are the most rigorous in documenting drug errors and the money they cost. Ordering prescriptions by computer dramatically reduces preventable errors.

Preventable errors include ordering doses that are too high or prescribing drugs to which a patient is allergic. Errors most often occur in sicker patients who take more than one drug, and they most commonly occur with antibiotics and pain killers. Errors that cannot be prevented include reactions to chemotherapy.

The first study, led by David Classen at LDS Hospital in Salt Lake City, found that:

- 2.43 drug errors occurred for every 100 admissions.
- Drug errors doubled the risk of death for a patient.
- Each error prolonged hospital stays two days and cost an extra $2,262 per patient.
- Preventable errors were cut by half with a computerized system that flagged unusual doses and allergies and adjusted for a patient's level of kidney function to arrive at the correct dosage. Poor kidney function can turn a normal dose into an overdose.

The second study, led by David Bates at Brigham and Women's Hospital, Boston, found preventable drug errors:

- Cost the hospital $2.8 million a year.
- Justify installing computerized prescribing systems, currently used in fewer than 10% of hospitals.

Bates estimates preventable drug errors cost the healthcare system $2 billion a year.

COVER STORY

Why planes take off with too little fuel

Reports show refueling system isn't fail-safe

By Julie Schmit
USA TODAY

The thought of it is terrifying: A jumbo jet packed with hundreds of passengers running out of fuel midflight.

Don't rule it out. The past nine years, 39 U.S. jets and smaller passenger planes have taken off or left the gate without enough fuel, a USA TODAY investigation has found.

In at least 16 cases, pilots didn't discover the shortage until the planes were airborne. Twice, a jumbo jet was over an ocean before the pilots realized they didn't have enough fuel to reach their destination.

No crashes or emergency landings occurred in the 39 cases. The flights didn't make the evening news. It's possible no one other than the pilots knew that something had gone wrong. Often, they returned to the airport they took off from to get more fuel. Sometimes, they made unplanned landings at other airports.

But such mistakes have led to near disasters. In 1983, an Air Canada Boeing 767 left Ottawa with less fuel than it needed. At 41,000 feet, its engines failed. It glided to make an emergency landing at an abandoned air strip. Two of the 69 on board were injured.

Refueling mistakes are rare, occurring in a tiny fraction of more than 60 million flights the past nine years. But the Air Canada captain says that's no comfort.

"It just shouldn't happen, not even once," says Bob Pearson, a 38-year pilot who now flies for Asiana Airlines.

The fact that it does happen shows how vulnerable airlines are to human error — a factor in seven in 10 crashes — despite elaborate systems of checks and double-checks.

The pilots — who are responsible for fuel loads — say simple things caused them to take off without enough fuel: fatigue, being rushed, math errors, forgetfulness, passenger distractions, sun glare on gauges. In one instance, a pilot said he was distracted by a fox on the runway.

Twenty-one of the 39 incidents came from reports that

Please see COVER STORY next page ▶

About this report

USA TODAY airline reporter Julie Schmit spent two months reporting today's Cover Story and the related stories and graphics on page 2B.

Schmit set out to answer a question many fliers perhaps never ask: How often do aircraft take off without enough fuel?

To get her story, Schmit studied safety reports and other documents obtained from the Federal Aviation Administration under the Freedom of Information Act. She obtained pilot reports filed voluntarily with the Aviation Safety Reporting System, an arm of NASA. And she interviewed more than 30 pilots, airline managers, FAA officials and safety experts.

The documents had their limitations. Some of the FAA records were too sketchy to use. The pilot reports obtained from NASA did not include names of pilots or airlines. The office deletes that information to preserve confidentiality. Sometimes other facts — routes, types of planes, number of passengers, specific dates — were missing.

But despite their shortcomings, the reports reveal how dangerous mistakes occur on U.S. airlines.

'Human performance' gets the blame for Amtrak crash

USA Today 22 Jan 98

y Peter Eisler
annett News Service

An ill-trained towboat pilot, ost in a foggy night when he ammed a barge into an unighted Alabama railroad ridge last September, got the fficial blame Tuesday for Amak's deadliest train wreck.

The National Transportation afety Board recommended tougher training, licensing and equipment requirements for towboat pilots.

"In this case, a human performance issue led directly to the most tragic accident in Amtrak history," board member John Lauber said of the crash that claimed 47 lives.

Lauber echoed other board members in blaming towboat pilot Willie Odom's mistakes partly to his employer, Warrior and Gulf Navigation, for instruction that was "informal, unstructured and relied mostly on on-the-job training."

But board members were unable to determine the extent of the firm's responsibility or the degree to which the accident reflects a more sweeping problem in the training and oversight of barge pilots.

Part of the problem, they said, was an incomplete investigation; part of it was the lack of barge accident records.

NTSB investigators said Odom, failing to properly use his radar or tie up when he got lost in the fog, never even knew he was near the 7-foot-high railroad bridge. He thought he'd hit a sandbar.

The barges knocked the span 38 inches off kilter, pushing a steel girder into the tracks. Minutes later, the first of three engines pulling Amtrak's Sunset Limited at 70 mph from Los Angeles to Miami hit the girder, tore the bridge apart, and flew more than 70 feet into the water. The lead engine spiked 45 feet deep into the bottom, spewing diesel fuel that burst into flames.

Industry Example

APRIL 19, 199
50 Cents

DOE probing 'human error' in shipping nuclear waste

Savannah River officials to meet with state regulator

By Frank Munger
Oak Ridge bureau

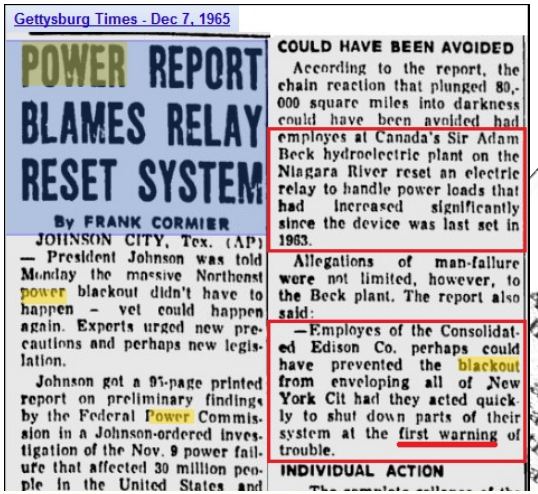
OAK RIDGE — The Department of Energy said Thursday "human error" was to blame for the waste shipment that arrived in Oak Ridge earlier this year with an abnormally high load of radioactive tritium.

Jim Giusti, a DOE spokesman at the Savannah River site in South Carolina, said a worker at a tritium-processing facility mistakenly put a piece of contaminated equipment into a box intended for low-level waste materials.

Giusti said a more detailed investigation is under way by Westinghouse, DOE's contractor at Savannah River, to assess the waste-handling system and come up with ways to prevent a recurrence.

"We take this very seriously," Giusti said. "DOE is looking at why this mistake was made."

Officials from the Savannah River plant are scheduled to meet next week in Nashville with Mike Mobley, Tennessee's top nuclear regulator, to discuss the incident and outline corrective measures. The shipment contained thousands of times more radioac-



Gettysburg Times - Dec 7, 1965

POWER REPORT BLAMES RELAY RESET SYSTEM

By FRANK CORMIER

JOHNSON CITY, Tex. (AP) — President Johnson was told Monday the massive Northeast power blackout didn't have to happen – yet could happen again. Experts urged new precautions and perhaps new legislation.

Johnson got a 95-page printed report on preliminary findings by the Federal Power Commission in a Johnson-ordered investigation of the Nov. 9 power failure that affected 30 million people in the United States and

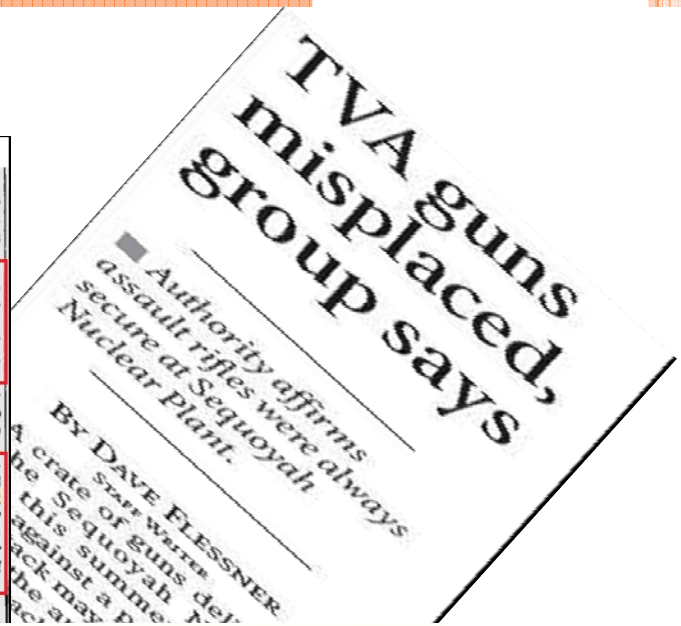
COULD HAVE BEEN AVOIDED

According to the report, the chain reaction that plunged 80,000 square miles into darkness could have been avoided had employes at Canada's Sir Adam Beck hydroelectric plant on the Niagara River reset an electric relay to handle power loads that had increased significantly since the device was last set in 1963.

Allegations of man-failure were not limited, however, to the Beck plant. The report also said:

—Employes of the Consolidated Edison Co. perhaps could have prevented the blackout from enveloping all of New York Cit had they acted quickly to shut down parts of their system at the first warning of trouble.

INDIVIDUAL ACTION



TVA guns misplaced, group says

Authority affirms assault rifles were always secure at Sequoyah Nuclear Plant.

By Dave Flessner
Staff Writer

USA TODAY · WEDNESDAY, OCTOBER 12, 2005 · 3A

Nation

L.A. goes through 3rd recent blackout

Mayor 'understandably concerned'

By Martin Kasindorf
USA TODAY

LOS ANGELES – The nation's second-largest city lost electrical power on a substantial scale Tuesday for the third time in four weeks, exasperating Mayor Antonio Villaraigosa in a blacked-out City Hall.

The City Council was in session when the lights went out. Backup power kicked in to keep parts of City Hall and police headquarters running.

Villaraigosa is "understandably concerned," mayoral spokesman Joe Ramallo said. Power was restored in most areas within three hours of the outage at 9 a.m. At midafternoon, about 100 buildings still were without electricity.

The blackout came after the mayor had already demanded answers about previous outages from Ron Deaton, general manager of the Los Angeles Department of Water and Power (DWP), the city-owned utility.

On Sept. 12, human error caused a 1½-hour outage to 2 million of the 4 million people in Los Angeles, Glendale and Burbank. The mayor said Deaton's explanation wasn't adequate and ordered a more thorough study.

Then on Sept. 23, another accident cut power to 40,000 homes and businesses.

Tuesday's outage at the DWP – the USA's largest municipal utility – knocked out service to 1,000 homes, businesses and government offices downtown, in adjacent Chinatown and in nearby neighborhoods. There was no word on the cause. Buildings that were affected included the 27-story City Hall and police headquarters.

The major blackout Sept. 12 unnerved some here because it came the day after the release of a letter from a suspected al-Qaeda terrorist in Iraq threatening an attack in Los Angeles. But the outage was blamed on a worker who cut three active power wires he thought had been disconnected.

Villaraigosa wrote to Deaton that the conclusions about the cause were "troubling because they confirm that the outage was the result of multiple errors and a lack of communication."

The failure on Sept. 23 started when a bank of transformers shut down. Power was restored in about five minutes.

Contributing: Wire reports

NATIONAL

Human error caused outage

March 1, 2008 | From Times Wire Reports

A power failure that plunged large parts of the state into the dark this week was caused primarily by human error, the state's largest electric company said. Florida Power & Light issued a report saying that a field engineer was to blame for the failure, which affected more than 1 million people.

NEWS

Human Error Blamed for Soviet Disaster

May 20, 1986 | WILLIAM J. EATON, Times Staff Writer

The chief designer of the Chernobyl atomic plant said Monday that he believes human error and not a technical failure led to the worst disaster in the history of the nuclear power industry. Ivan Y. Yemelyanov, a non-voting member of the Soviet Academy of Sciences, also said in an interview with Western reporters that the Soviet Union does not build containment domes over its reactors because they do not guarantee safety and can lead to a false sense of security.

Single worker caused massive power outage across Southwest, power company admits

BY NINA MANDELL / DAILY NEWS STAFF WRITER / Friday, September 9, 2011, 12:51 PM

A A A

NEWS

S.F. Blackout Blamed on Human Error and Mechanical Failure

December 17, 1998 | *From Associated Press*

The San Francisco blackout that affected more than 1 million residents was triggered by a combination of mechanical failure and human error, Pacific Gas & Electric Co. said Wednesday. Investigators from PG&E continue to probe the causes of the Dec. 8 outage that shut down San Francisco and parts of San Mateo County.

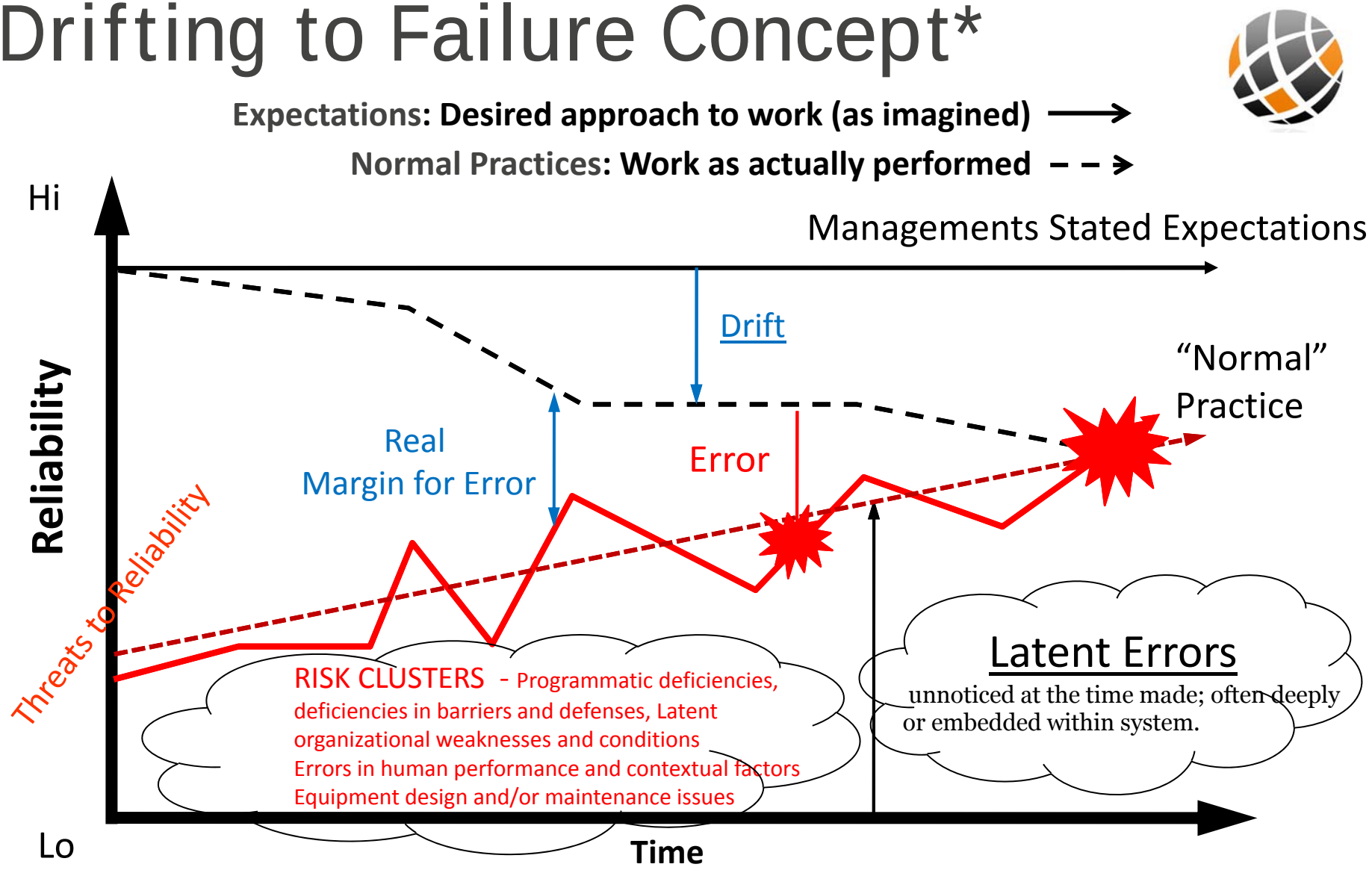
NEWS

PG&E Wraps Up Probe of Power Outage, Blames Human Error

January 24, 1999 | *From Associated Press*

Human error, not a system flaw, remains the prime reason 2 million San Francisco area residents lost power in last month's massive blackout, Pacific Gas & Electric Co. said after completing an internal investigation. The investigation uncovered no significant glitches in operations or in the design of San Francisco's electric transmission system, the San Francisco Chronicle reported Saturday.

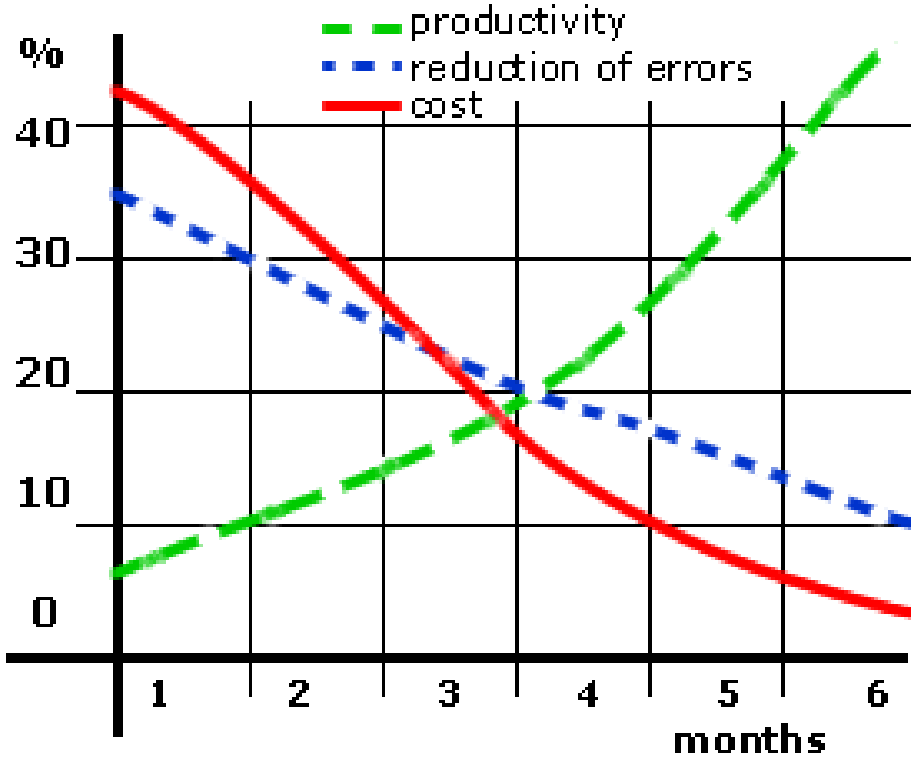
Drifting to Failure Concept*



* Adapted from Sidney Decker's Deviation from Normal and Tony Muschara's Error Management Approach

Human Drift Controllable Factors

1. Work Environment
2. Equipment Design
3. Procedures
4. Communications
5. Job Aids
6. Task Design
7. Training
8. Supervision
9. Individual Differences
10. Job Design



Performance Modes

GEM
(Generic Error Model)

Skill Base - highly practiced actions (routine activities) executed from memory... errors made by skilled personnel while performing familiar tasks for which they are essentially experts or well practiced. Typical Error Rate - 1/10,000

Rule Base - performing a task based upon selection of rules from recognition... result when a "rule" (from training, procedure, etc.) is misapplied or a shortcut is taken. Typical Error Rate - 1/1,000

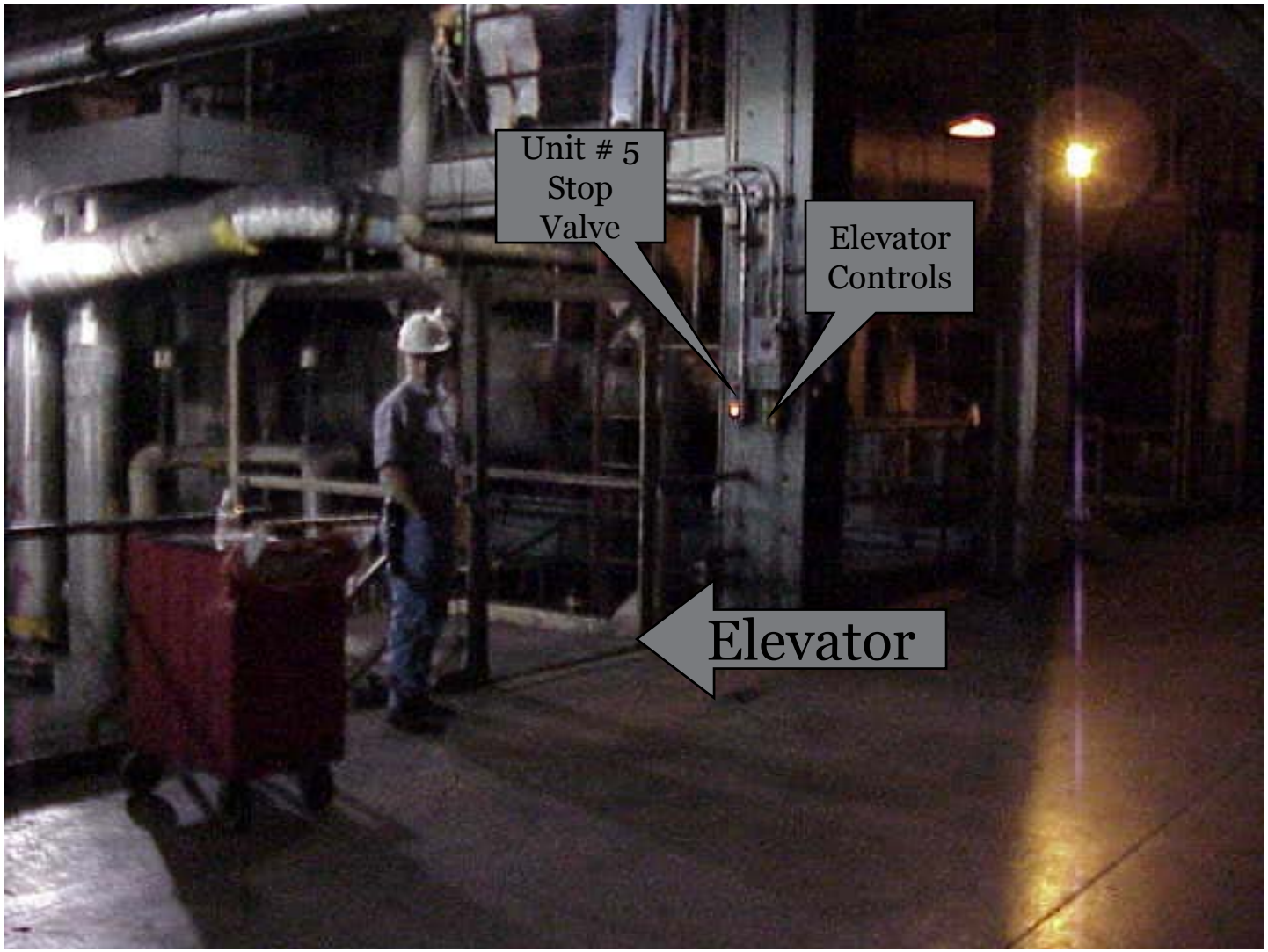
Knowledge Base - performing totally unfamiliar tasks based upon your understanding or knowledge of a situation. Error Driven... Behavior in response to a totally unfamiliar situation relying on one's understanding. Typical Error Rate - 1/2

Latent Organizational Weaknesses

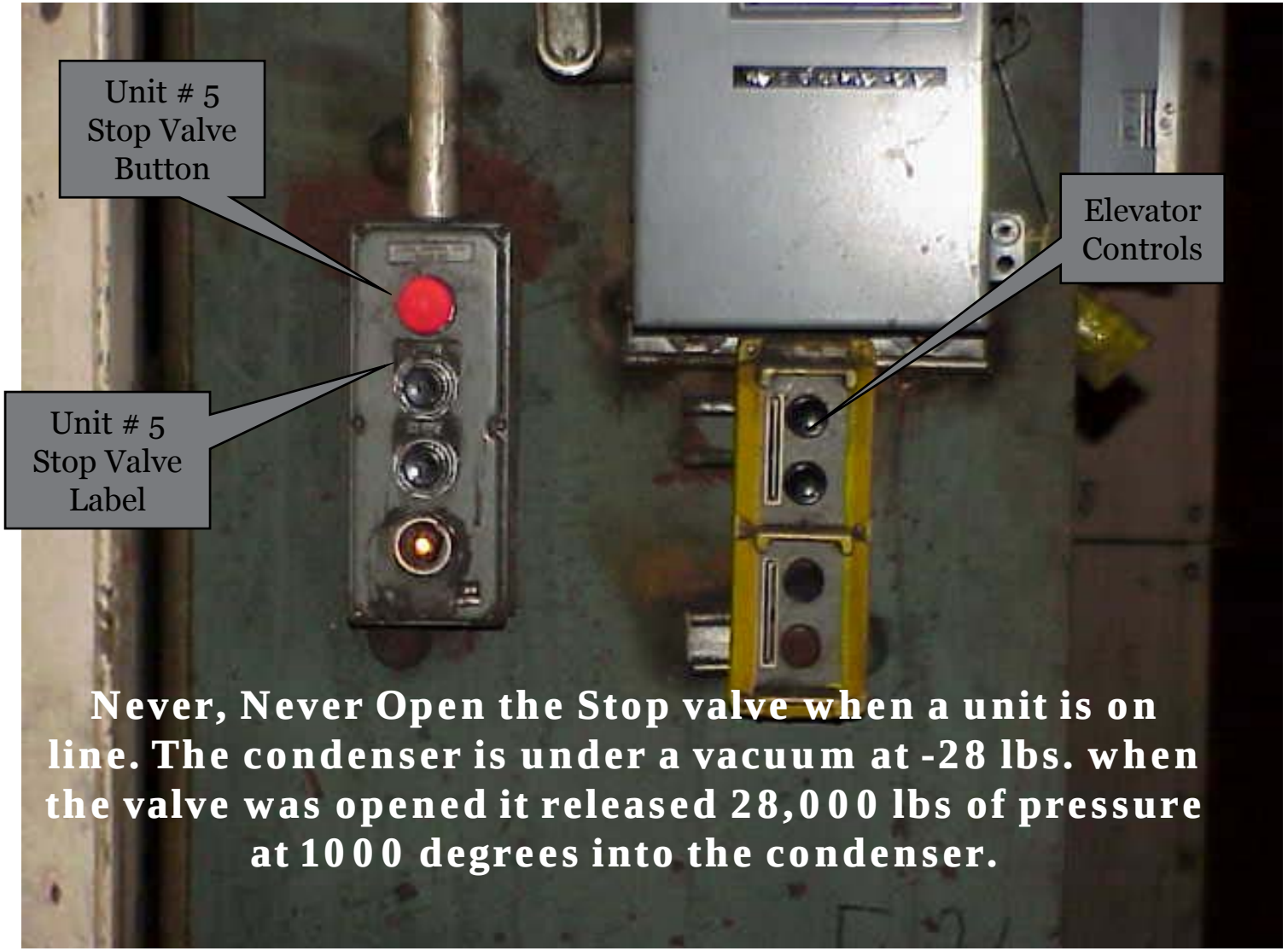
- Hidden deficiencies in management control processes or values creating workplace conditions that can provoke errors (precursors) and degrade the integrity of defenses (flawed defenses).

Fossil Plant Case Study

Unit # 5 Stop Valve



Wrong Button pushed



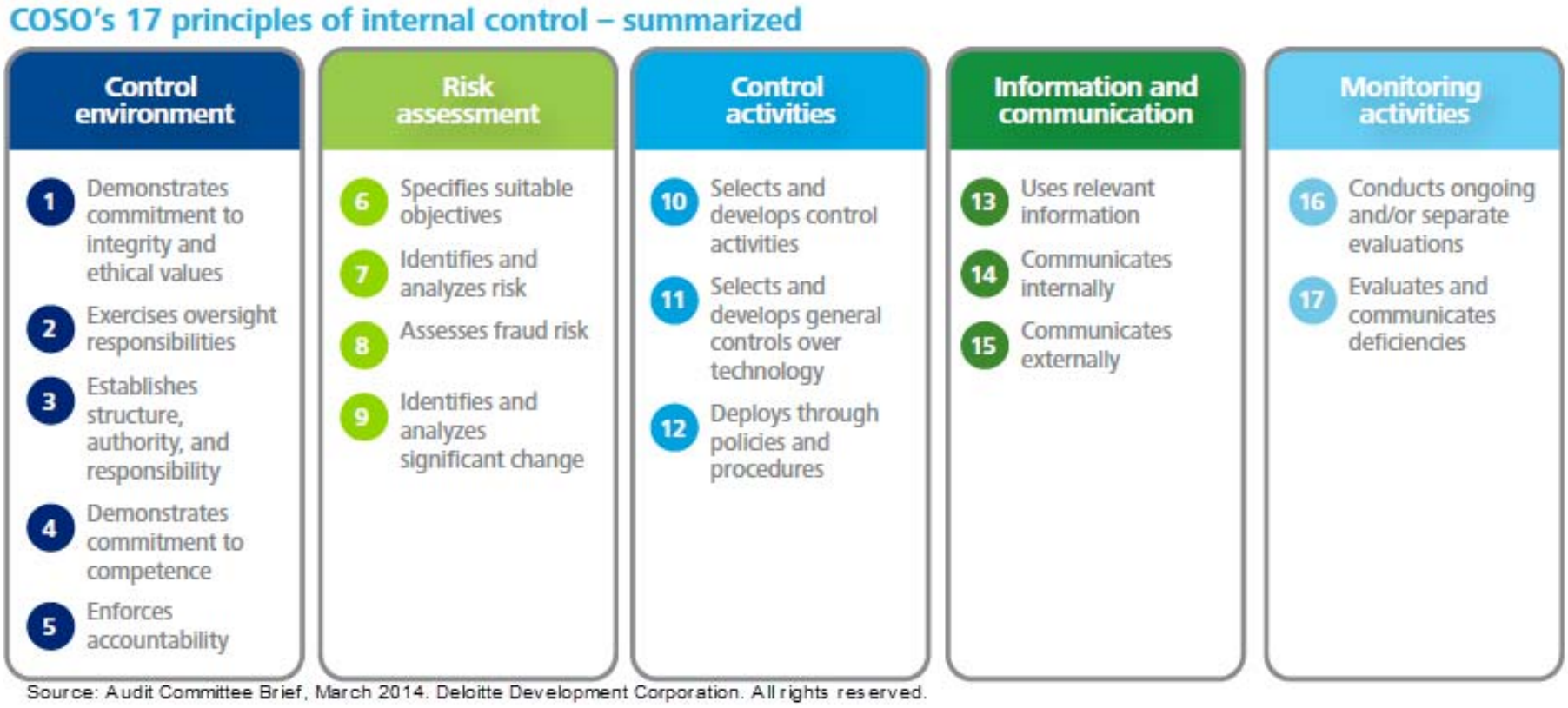
The Results:


600 Dollars to fix
210 Valve
210 Valve
$700,000 to repair Unit Condenser and $1.2 Million in lost generation = $1.9 Million Dollars

Internal Controls System Framework

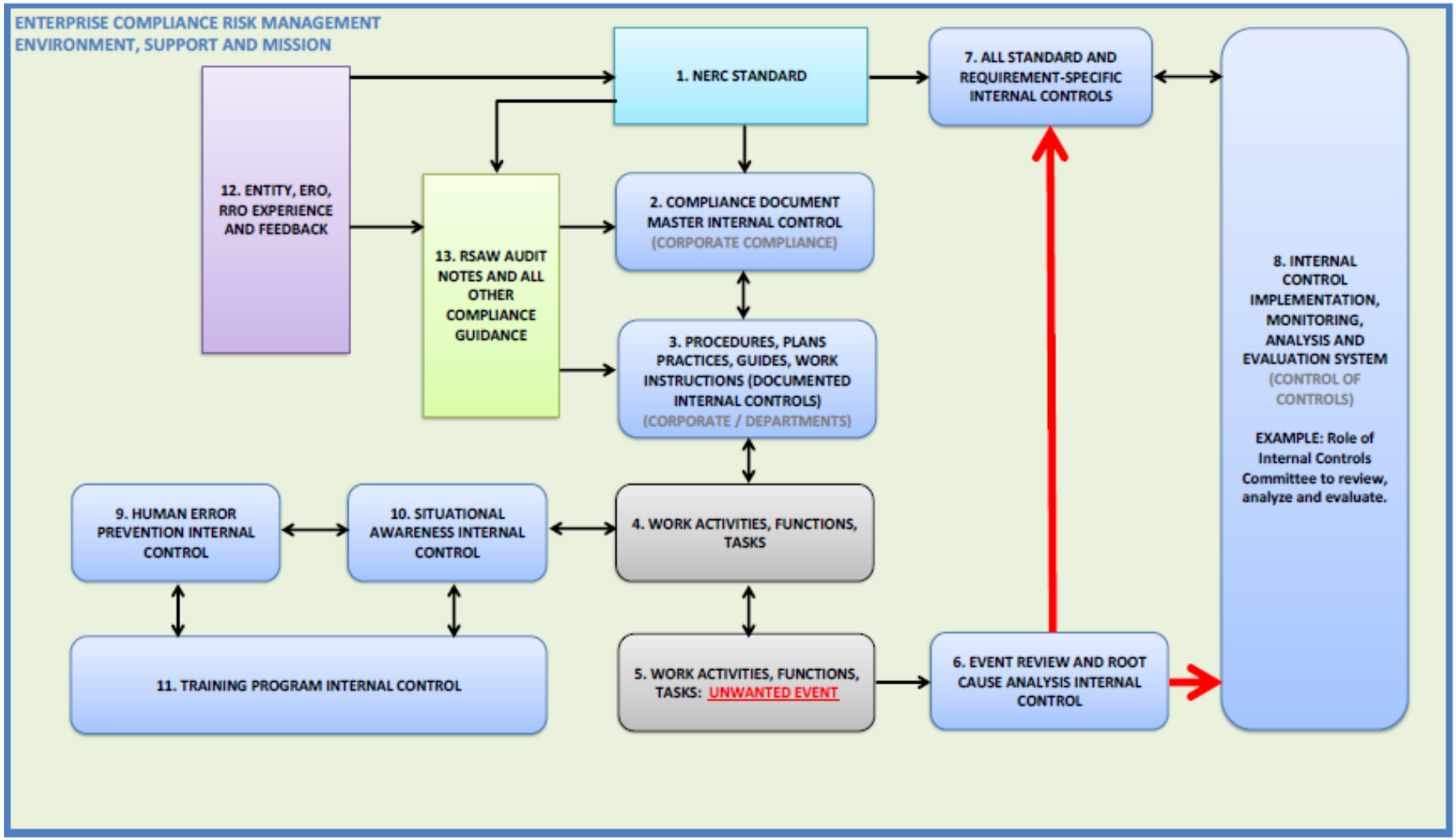
Adapted from COSO and GAO

COSO's 17 Principles



The Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Example Integrated framework



Types of Risk

Inherent

- Dependent on organization's functional registrations
- Capability, materiality, system design, configuration, size, location, etc.

Control

- Risk that a control will not meet the desired objective of exceptional operational and compliance performance.

Detect

- Risk that a control failure goes unnoticed

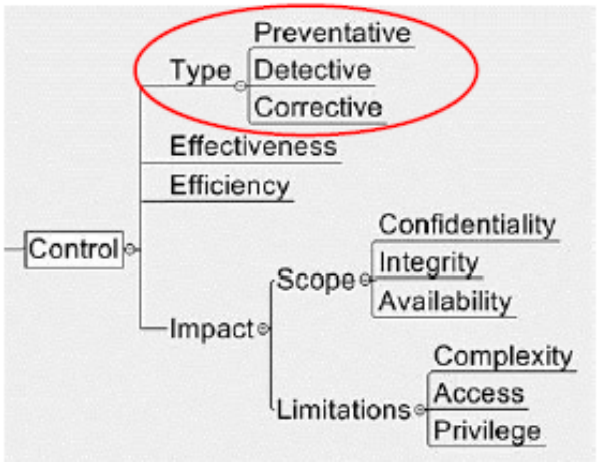
Response to Risk

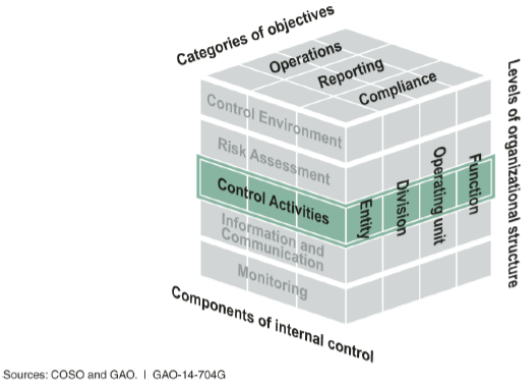
Acceptance	• No action taken based on insignificance of risk
Avoidance	• Action taken to stop the operational process or the part of the process causing the risk
Reduction	• Action taken to reduce the likelihood or magnitude of the risk
Sharing	• Action taken to transfer or share risks across the entity with external parties

Risk Control Activities Defined

- Integrated business management practices (addressing technology, people, policies, and procedures) that reflect the vision of the control environment of an organization.

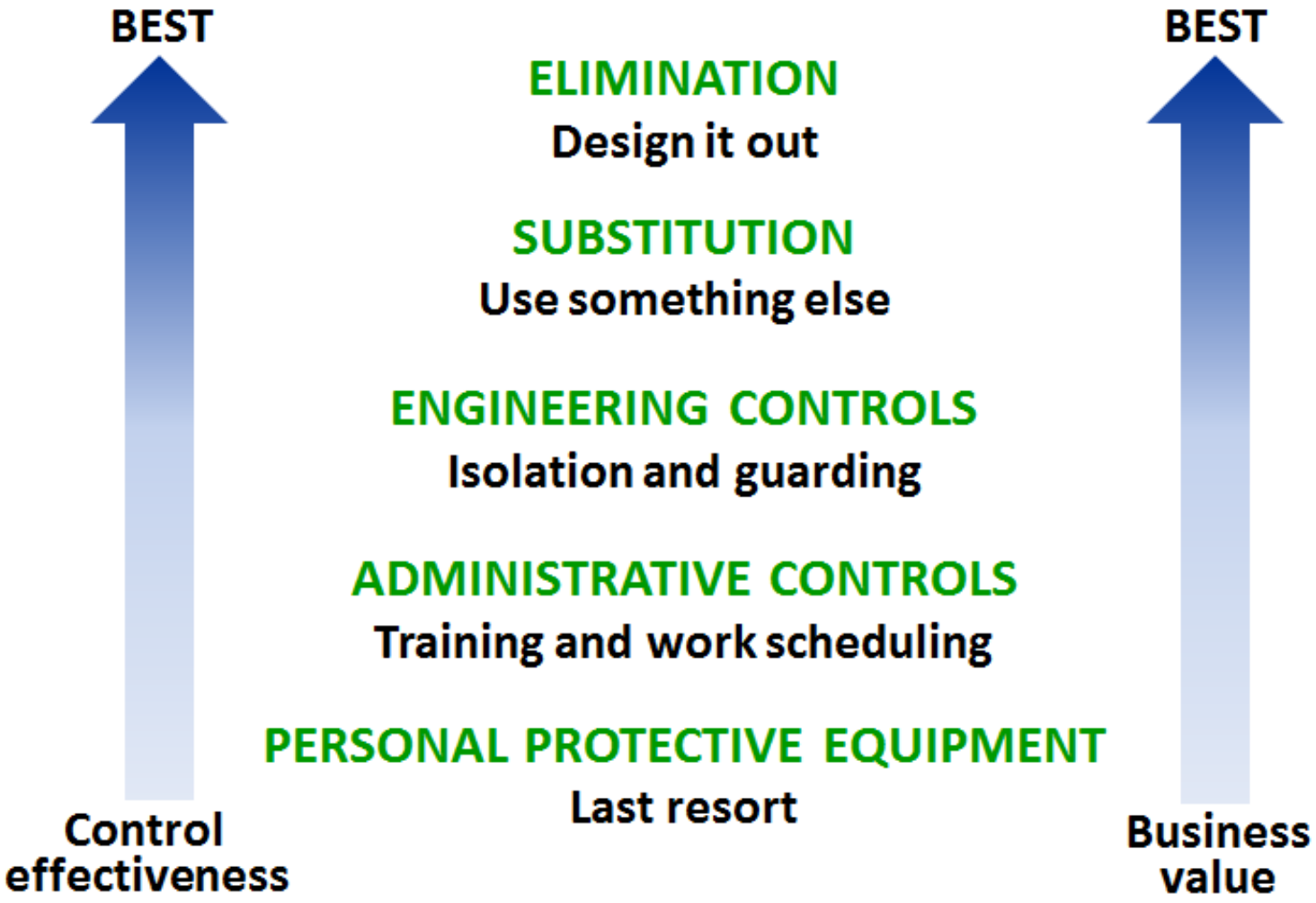
- Well-designed control activities consist of overlapping complementary control frameworks and interrelated components striving to meet the organizational objectives





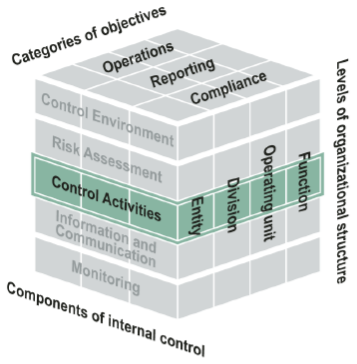
Sources: COSO and GAO. | GAO-14-704G

Control Hierarchy



Preventive Control Activities

- Proactive control design to discourage non-compliance with Reliability Standard
- Example: Documented Process requiring development and maintenance of training schedule
  - Process would include all required training, scheduled to ensure completion prior to dates required by the applicable reliability standard
  - May use automated training tracking tool (notifies individual of scheduled training, reminds them to complete training, and notifies management to take action if training is not completed prior to the deadline)



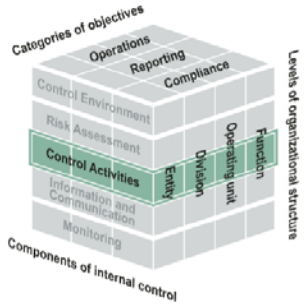
Detective Control Activities

- Designed to find errors or irregularities and support effective compliance

- Example: Documented process requiring periodic review to identify any required training not completed as scheduled, as well as training not completed per reliability standard requirements

  - Quarterly review of completed training records to identify individuals who have not completed training by the required deadline

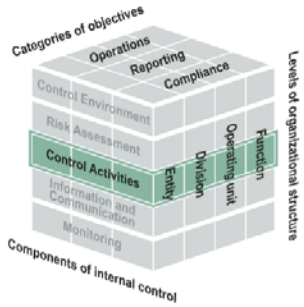
  - Documentation and utilization of an event review and root cause analysis process to determine cause and effects surrounding an unwanted event



Corrective Control Activities

- Designed to assess instances of non-compliance and return to a state of compliance

- Example: Automation of an Automatic Voltage Regulator (AVR) status indication
  - Would cause an alarm in the TOP's EMS, indicating an AVR status change from Auto to manual on a particular generator unit
  - Would provide notification to the TOP of an AVR status change within 30 minutes as required by VAR-002



Control Measure?

CAPITOL ALERT MAY 29, 2015

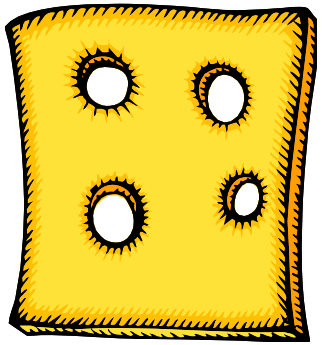
California Senate offers 24-hour rides for lawmakers too drunk to drive

BY ALEXEI KOSEFF AND JIM MILLER
akoseff@sacbee.com

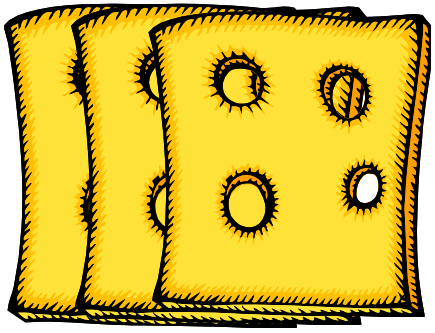
California Senate officials earlier this year hired two part-time employees to provide late-night and early-morning rides for members while they are in Sacramento, a 24-hour service that follows high-profile drunken driving arrests involving lawmakers in recent years.

Why Controls in Depth are Important

Even the best controls are fallible and can have holes…..

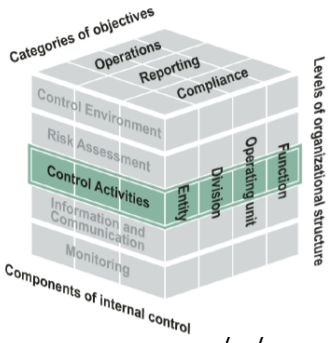


Multiple Complementary Risk Controls Reduce the likelihood of an event…



Complementary Control Activities

Procedure/ Process	Control	Control Activity	Control Type
Program Documents (Procedures)	Work Order	Checklist followed and completed, exceptions noted, follow-up notes signed	Primary Control
	Supervisory Review	Review for completeness and accuracy, follow-up actions closed or scheduled to be completed, signed	Secondary Control
	Management Oversight	Periodic sampling of work orders to determine program is being completed and properly reviewed	Tertiary Control



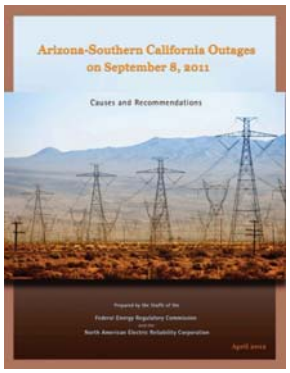
Residual Risk

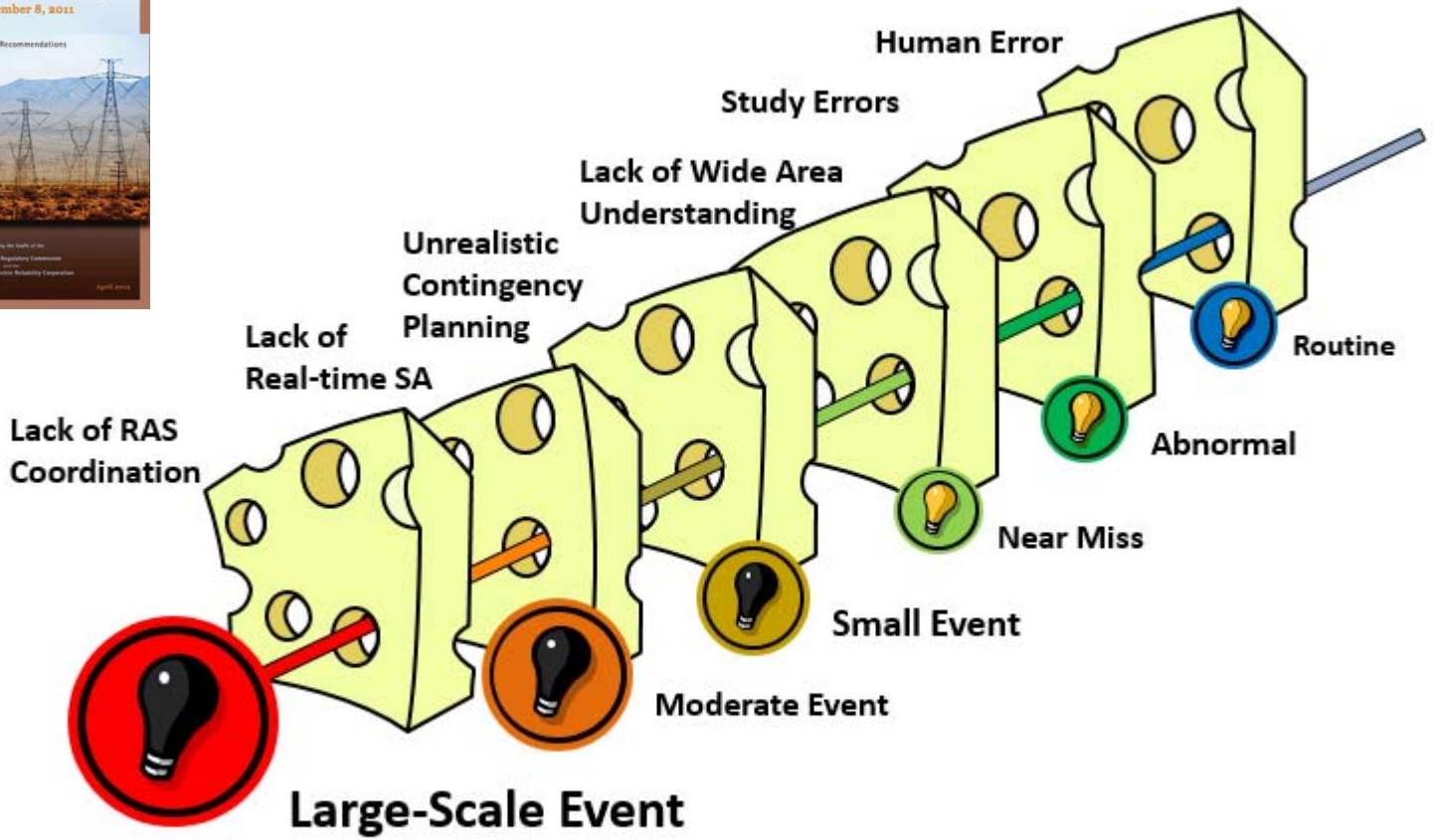
- Residual risk is the level of risk after evaluating the effectiveness of controls
- there is always remaining residual risk after any given risk response
- Acceptance and action should be based on residual risk levels.

Validating your results

- Impact Factor X Frequency Factor = INHERENT Risk Factor
- Inherent Risk Factor X Control Factor = RESIDUAL Risk Factor
- The Higher the residual risk factor the more ineffective the controls

Case Study - 2011 SW Blackout



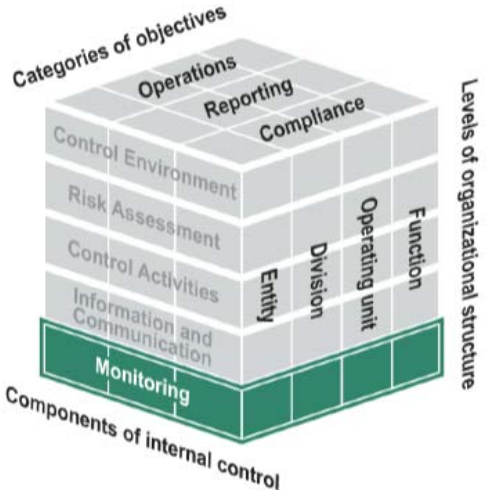


* Adapted from Human Error, by Dr. James Reason

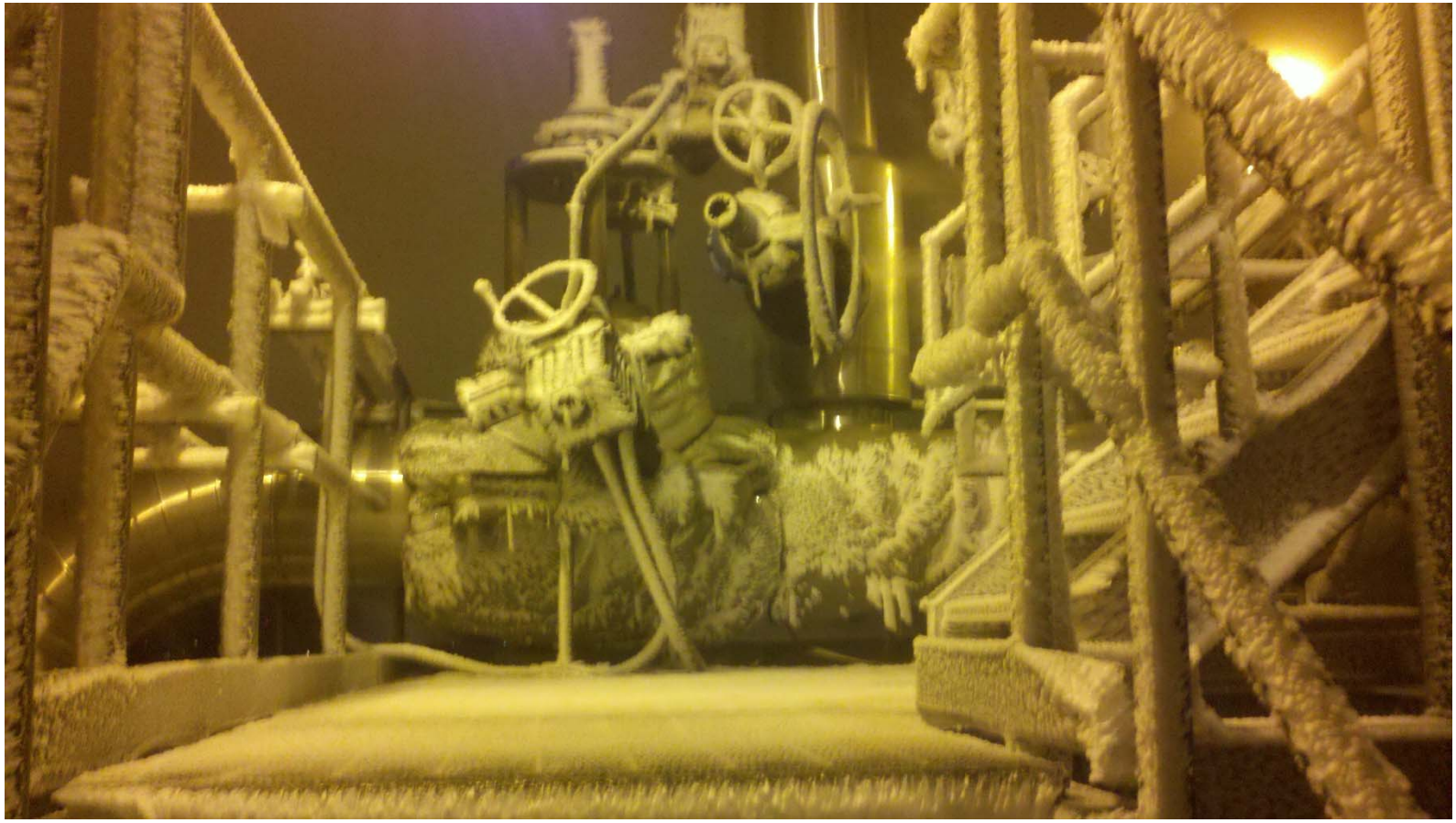
Monitoring (Sustainability)

- Ongoing and periodic evaluations
- Determines the effectiveness of the System
- Identifies deficiencies and corrective actions
- Determines the presence, functionality, and integration of controls
- Can be manual (e.g. periodic management review) or automated (e.g. alarms, messages etc.).

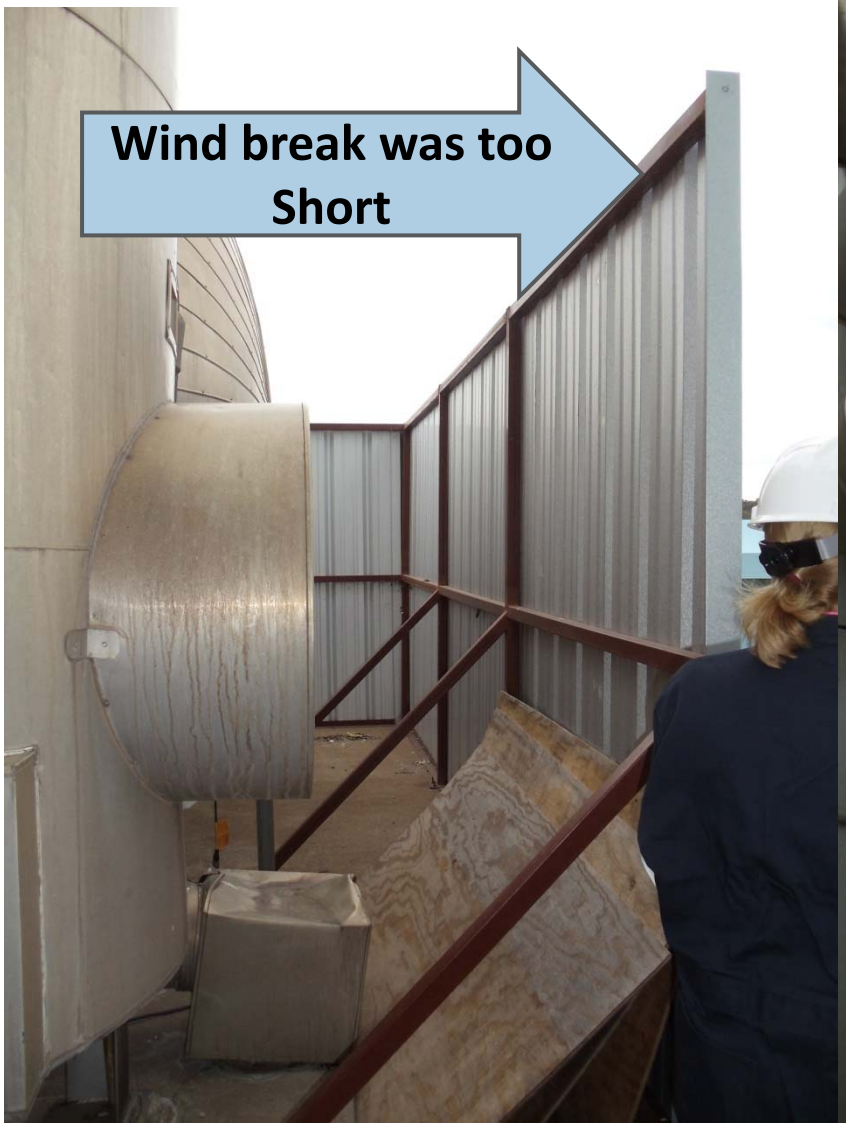
- Know what to expect
- Know what to look for
- Establish a baseline
- Evaluate the results
- Corrective actions



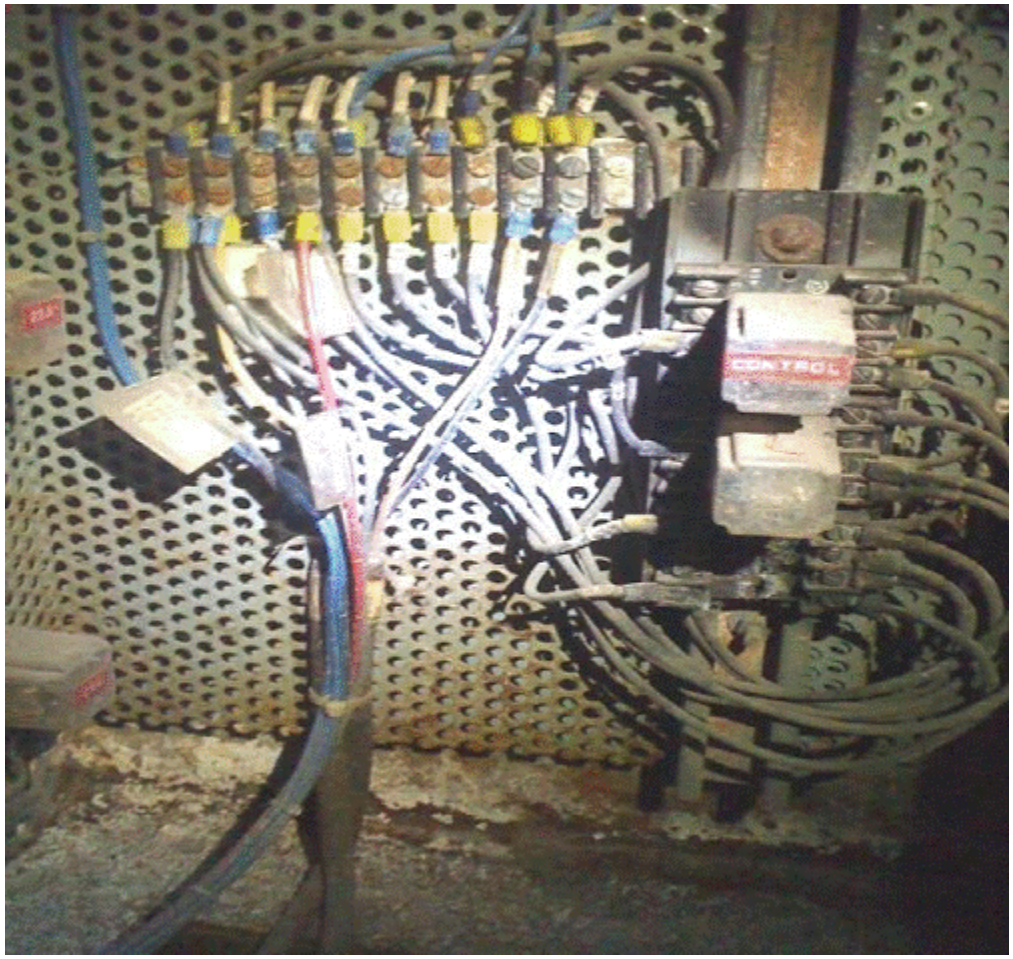
2011 Cold Snap Case Study



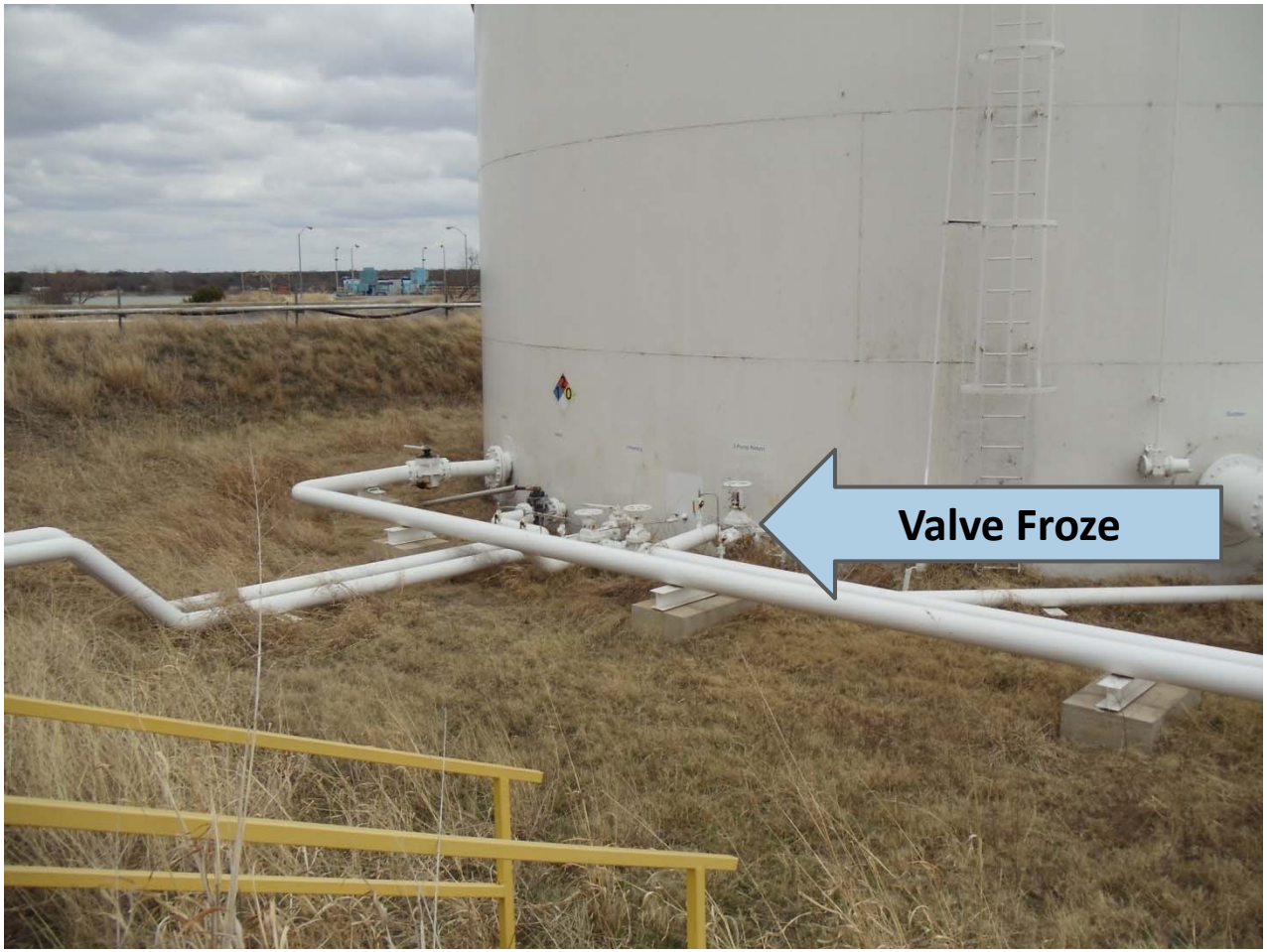
Wind Break Design



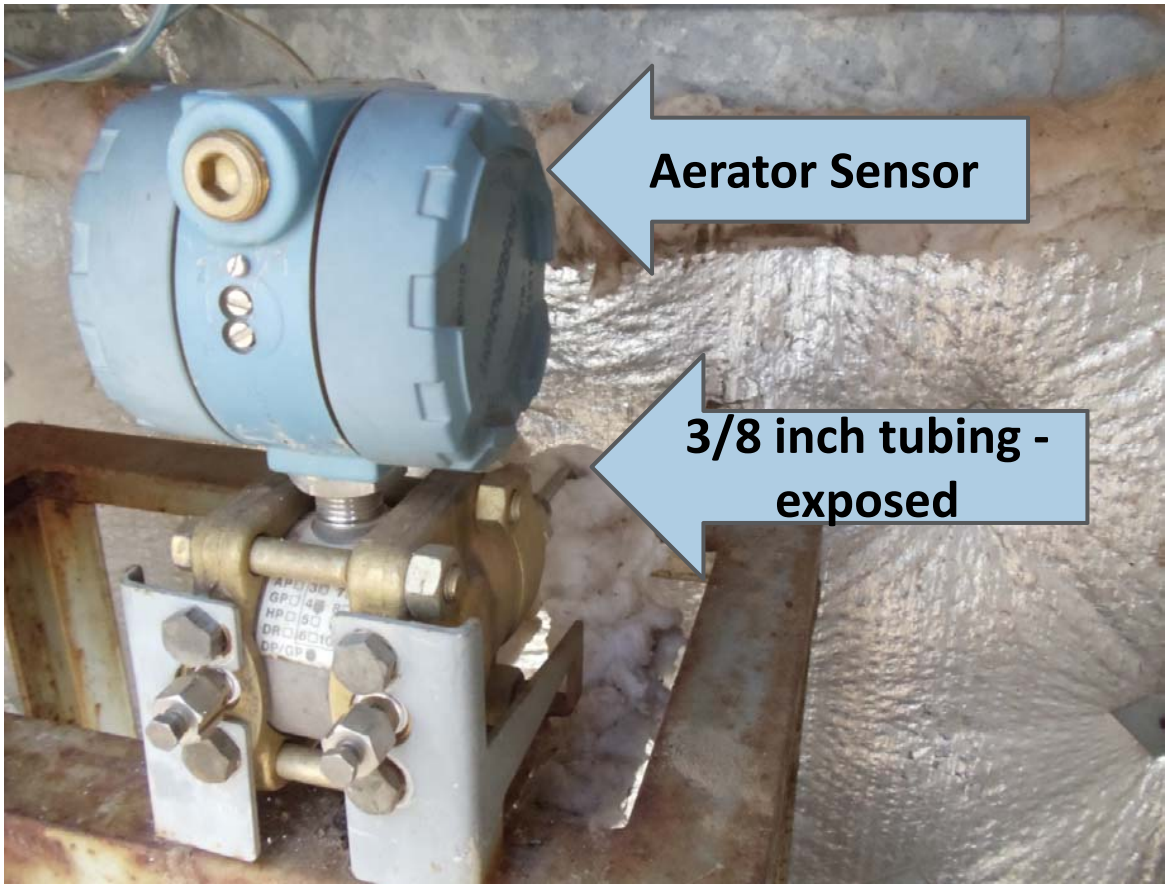
Corroded Freeze Protection Panel



Fuel Transfer Valves



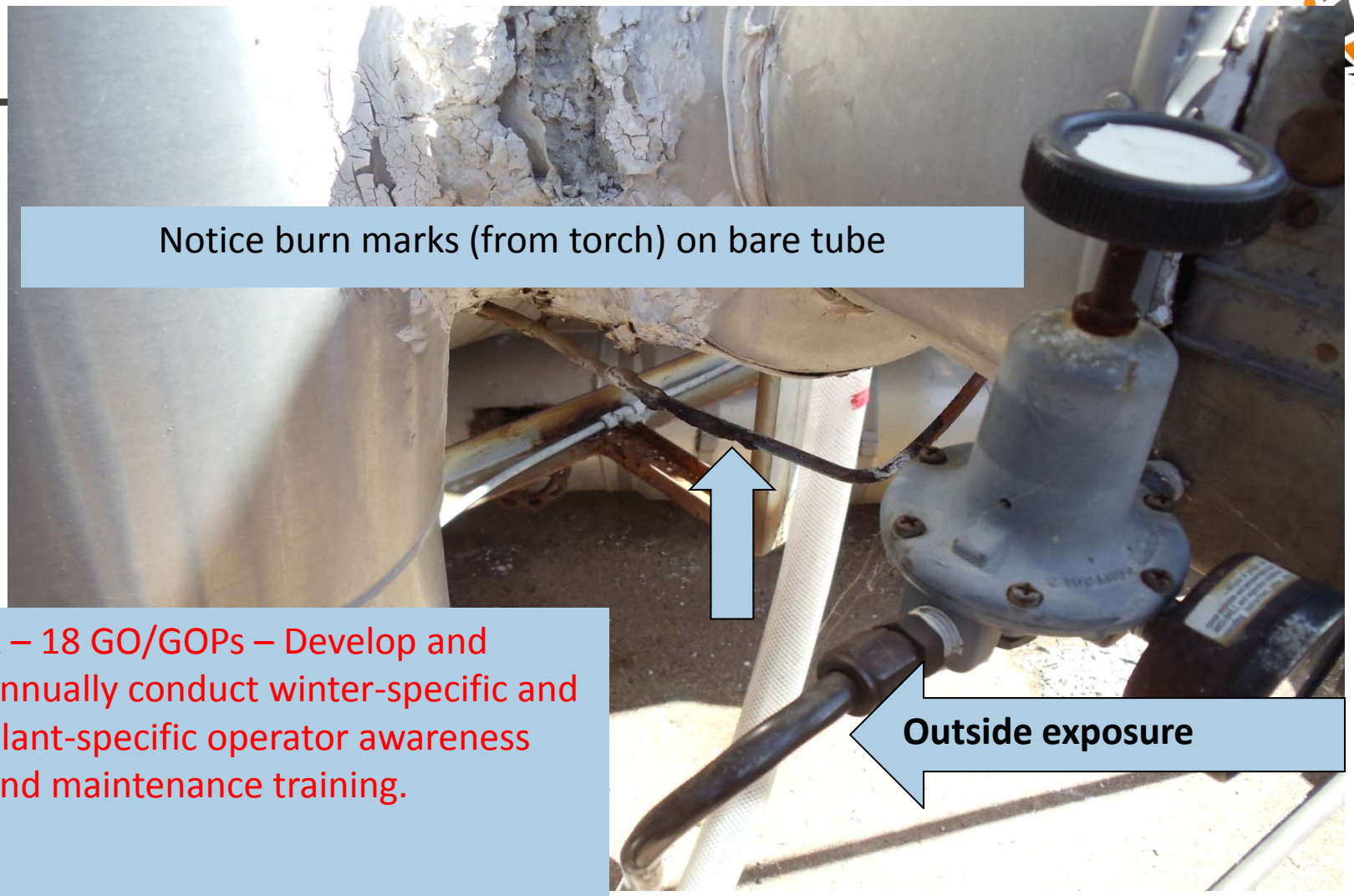
Frozen Sensor



Inadequate Insulation

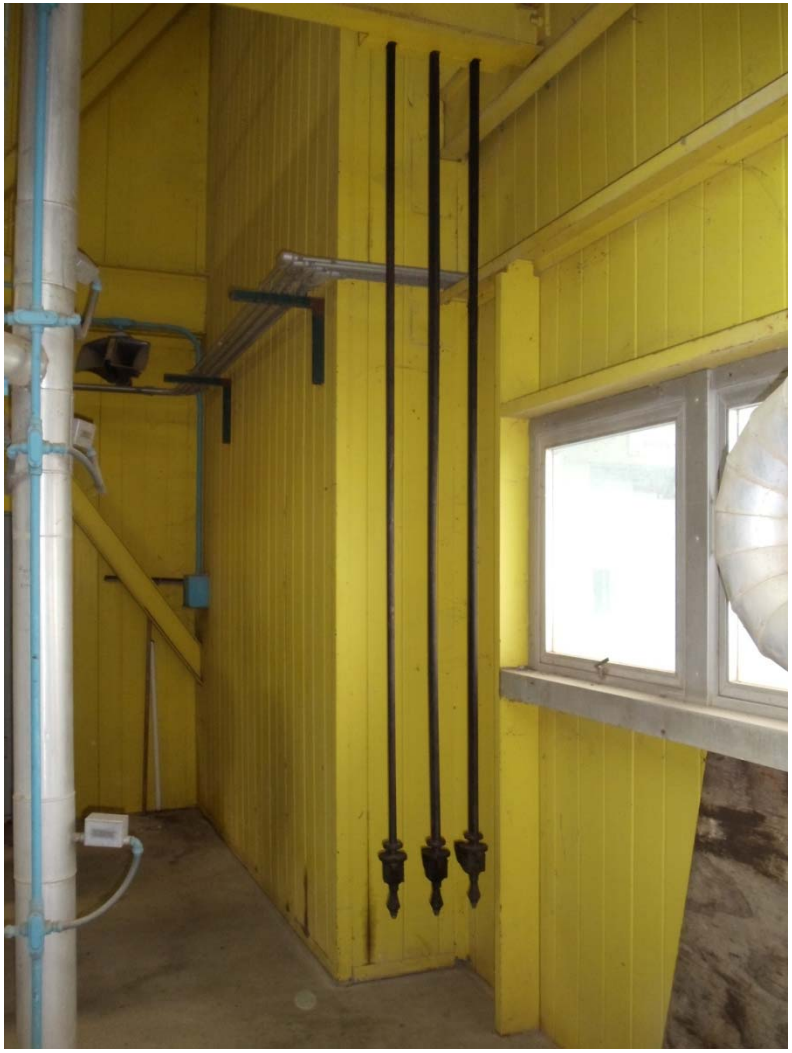
R-16 GO/GOPs – inspect and maintain thermal insulation on all units.

L



R – 18 GO/GOPs – Develop and annually conduct winter-specific and plant-specific operator awareness and maintenance training.

Oil Burning Wands

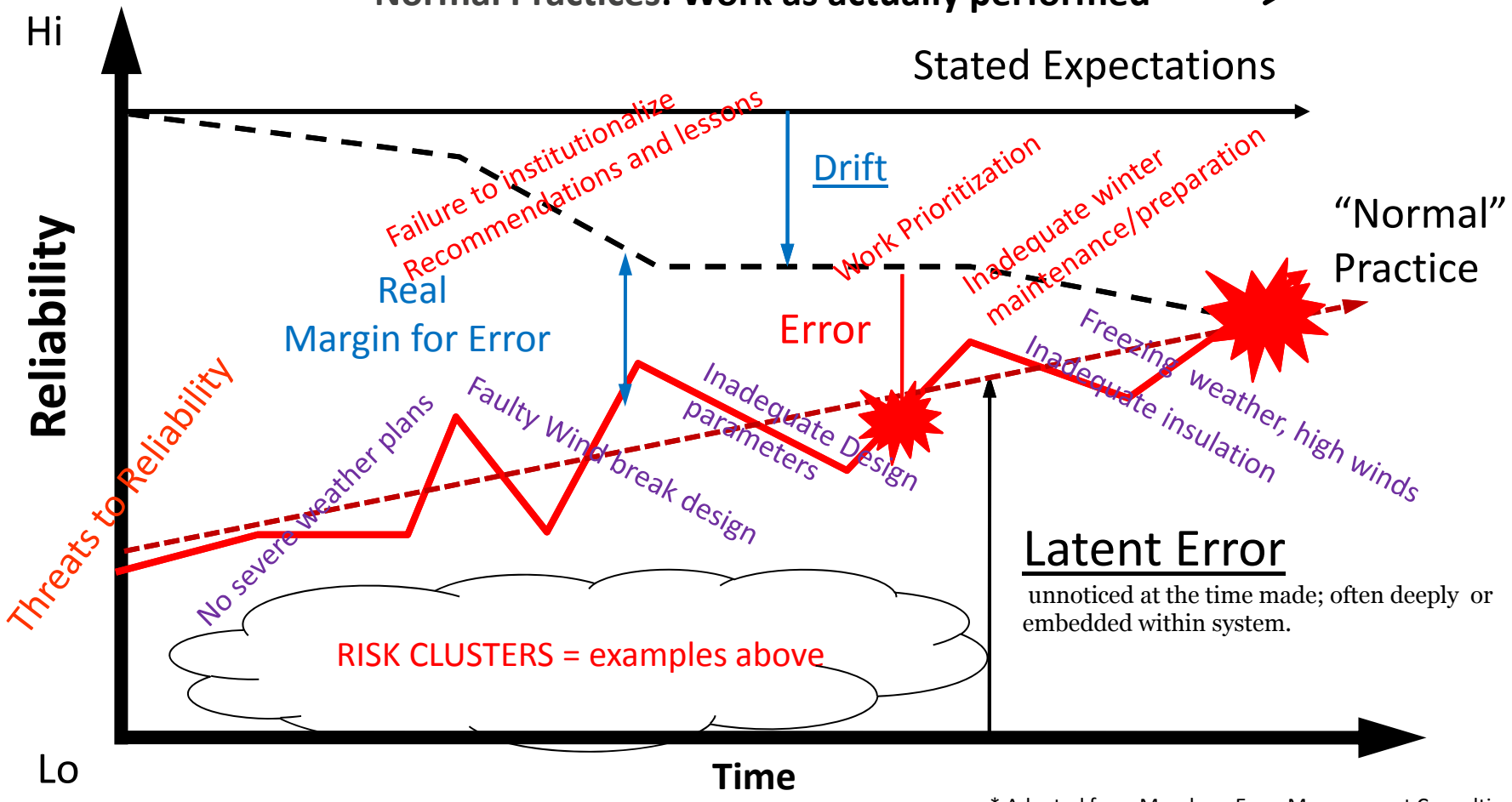


R – 6 TOs, BAs, and GO/GOPs – Verify that units that have fuel switching capabilities can periodically demonstrate those capabilities

Cold Snap Event Drift to Failure*

Expectations: Desired approach to work (as imagined) →

Normal Practices: Work as actually performed - - →



* Adapted from Muschara Error Management Consulting, LLC

2011 Cold Snap Event

When the <u>wrong set</u> of circumstances line up, major events occur…

* Adapted from Dr. James Reason, Human Error 1990

Countermeasure – Critical Transmitter Freeze Protection

With heat trace energized:

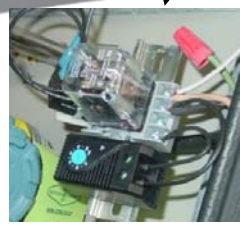
Light lit steady => circuit on, box at set temperature

Light flashing => circuit on, box below set temperature

Light out => no power available to heater

Local thermometer for cold weather IOW

Circuit monitors heater status & temperature



Box is also externally blanketed

Takeaway: **Local thermometer is installed for the IOW and a beacon light is utilized for heater health indication.**

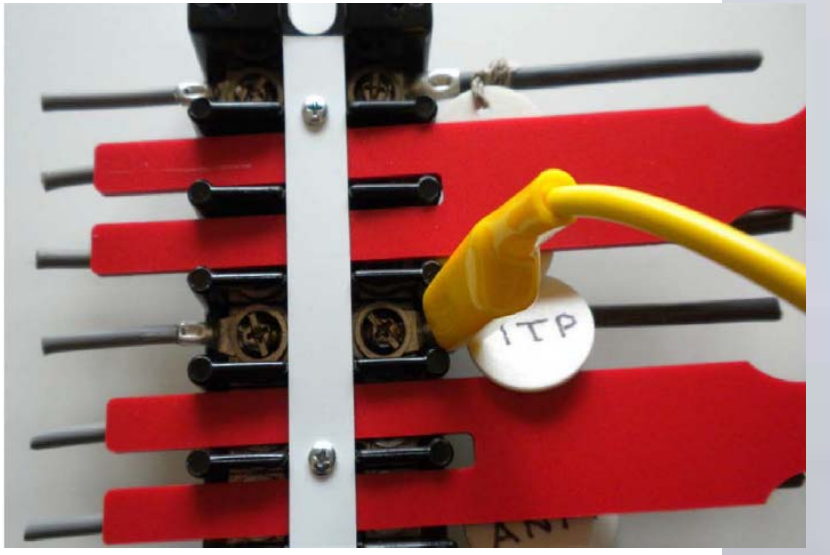
Countermeasure - Critical Transmitter Freeze Protection

Lights of transmitter boxes are easy to see far away and we can quickly dispatch someone to check when it flashes

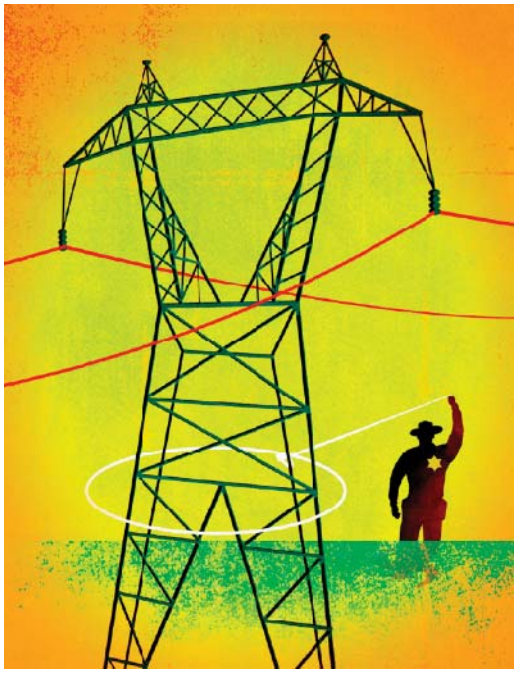
Insulation blanket is installed to keep the box warm

Takeaway: **Numerous events have been caught by operators observing the warning beacon lights after the installation was completed.**

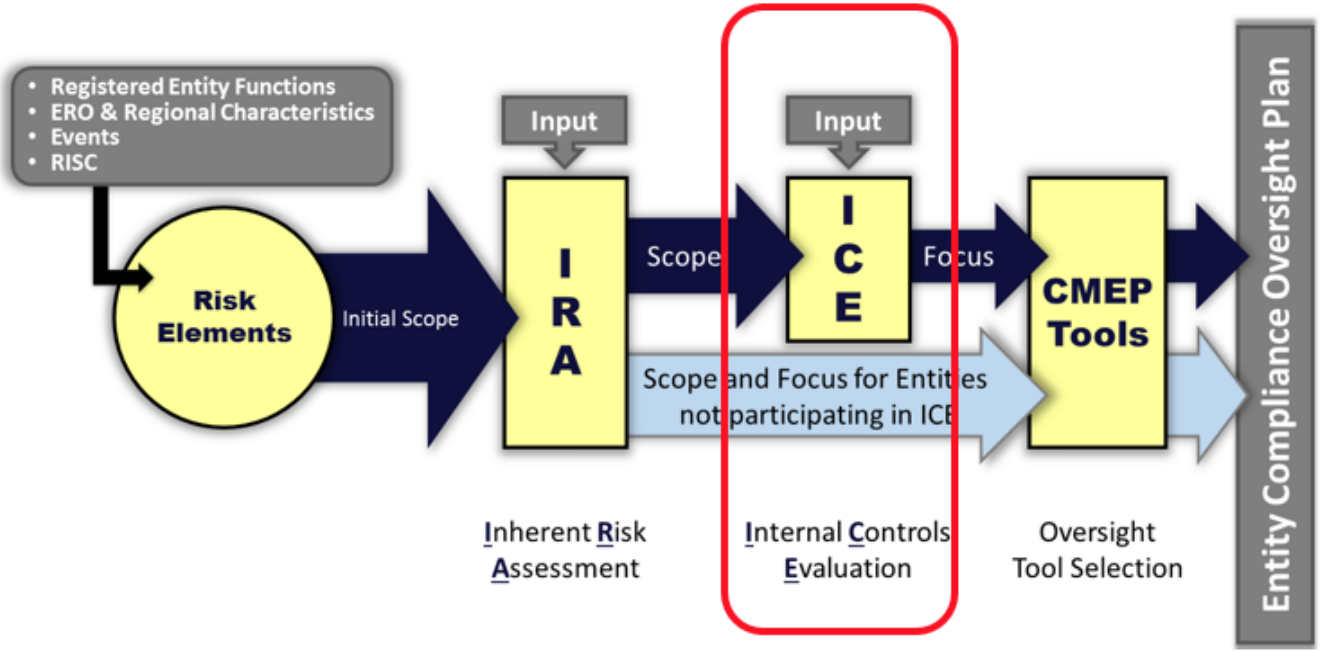
Smart Controls



What to Expect From Regulators



ERO Risk-Based Monitoring Framework



Regulators Expectation

- Organizations defines its own procedures and management practices around its risks – establishing controls to mitigate and manage Risk.
  - Determine Greatest Risks
  - Develop and implement model controls
  - Evaluate quality and vigor of controls
  - Self-monitor with responsibility/accountable governance
  - Documentation of controls
  - Demonstrate competence of control

Objective of ICE

- The Compliance Enforcement Authority (CEA) (e.g. WECC) is ultimately responsible for determining whether a registered entity has implemented an internal control program containing sufficient controls that provides reasonable assurance of compliance with Reliability Standards in the service of reliability.

- The CEA will make this determination by understanding the BPS risks to which the registered entity is susceptible and how the registered entity manages or mitigates those risks.

Purpose of ICE

- ICE results help the CEA determine engagement scope and may impact sampling and testing during audit
- Compliance is measured by adherence to the standards not effectiveness of controls

What Regulators Look For

- The 5 key components of IRCS are operating together in an integrated manner
- Controls are designed individually and in combination with other controls so they are capable of achieving an objective and address related risks.
- Controls are effectively cataloged and documented
- Effectively and dynamically implemented to enable the objectives
- Effectively and dynamically monitored for competence

GAO Factors

Key Questions

Key Questions in Control Identification and Walkthrough Phase

3.1.1.2

- Has the entity established internal controls to address the standards and requ associated with the IRA risk?
- What internal controls are most im to monitor to ensure applicable NI Reliability Standard Compliance?

3.1.1.3

- When applied does the control the intended result?
- Is there sufficient, credible evide obtain reasonable assurance tha control produces the intended r

3.1.1.4

- Does the entity monitor the con
- Can the CEA use the results of th monitoring to reduce complianc monitoring efforts?

Key Questions for Testing Effectiveness of ICP Phase

3.2.1.2

- What types of internal controls has the entity identified in the ICP?
- Is there a blend of preventative, detective, and corrective controls to address each risk?

3.2.1.3

- Is the ICP designed
- Is the ICP
- Is the inte mitigated
- Does the correct d Reliability Requirem

Key Questions for Finalizing ICE Conclusions

- Do the internal controls mitigate the risks identified in the IRA?
- Where the internal controls do not completely mitigate the risk, should correction of the internal controls be encouraged, rather than focus on individual NERC Reliability Standard testing?
- How does the entity's internal controls inform the compliance oversight plan for this registered entity?

Risk Management Tools that Can Help

Olfactory "Fatigue" Adaption "you cannot smell your own house"

A useful concept to understand how an organization can benefit from independent reviews of important systems.

Cost of Regulation

AAF – A Regulatory Flurry: The Year in Regulation, 2013

Regulatory Compliance Costs of 30 Large Companies (in millions)			
Company	Total	Market Cap	Costs/Market Cap
Bank of America	$1,700	$166,000	1 percent
Wells Fargo	$900	$239,000	0.4 percent
JPMorgan Chase	$706	$217,000	0.3 percent
U.S. Bancorp	$80	$73,000	0.1 percent
PNC	$314	$41,000	0.7 percent
Metlife	$149	$60,000	0.2 percent
ExxonMobil	$814	$440,000	0.2 percent
ConocoPhillips	$1,531	$86,000	1.7 percent
Marathon Petroleum	$584	$27,000	2.2 percent
Chevron	$1,403	$239,000	0.6 percent
Valero	$333	$27,000	1.2 percent
Hess	$224	$28,000	0.8 percent
AEP	$2,389	$22,000	10.9 percent
Southern	$4,729	$36,000	13.1 percent
Duke	$5,740	$48,000	12 percent
Alcoa	$532	$11,000	4.8 percent
GE	$1,200	$282,000	0.4 percent
Honeywell	$1,038	$71,000	1.5 percent
Dow	$754	$54,000	1.4 percent
Boeing	$865	$102,000	0.8 percent
Lockheed Martin	$950	$47,000	2 percent
GM	$250	$56,000	0.4 percent
IBM	$400	$203,000	0.2 percent
Ford	$125	$60,000	0.2 percent
United Technologies	$230	$103,000	0.2 percent
3M	$86	$94,000	0.1 percent
Pfizer	$1,604	$199,000	0.8 percent
Merck	$498	$146,000	0.3 percent
Abbott Labs	$75	$59,000	0.1 percent
Aetna	$80	$25,000	0.3 percent
Totals:	$30.2 billion		Average: 1.9%

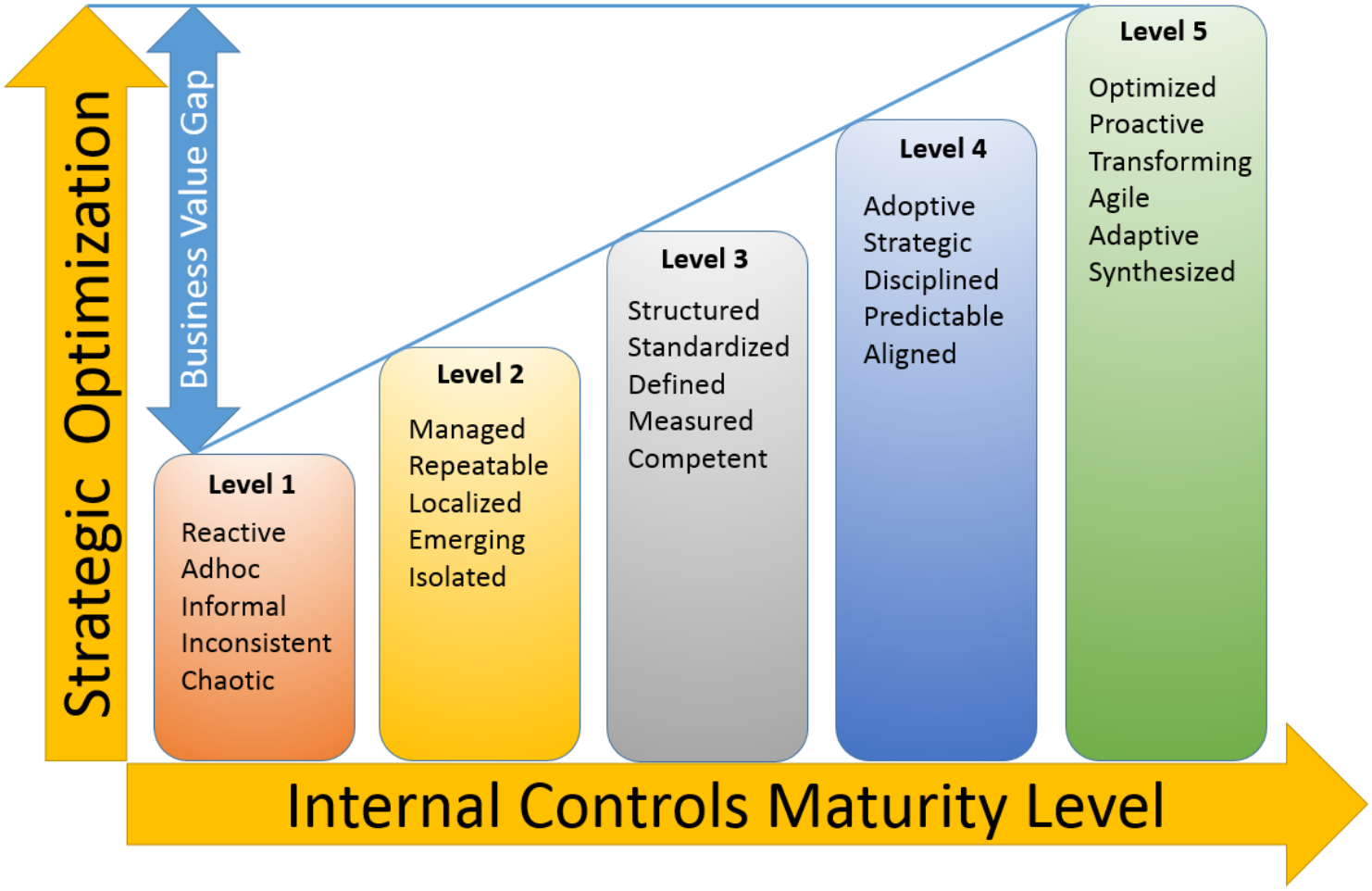
Internal Risk Control Maturity Assessment

- A method to measure the level of organizational readiness and experience in relation to Enterprise Risk Management and Internal Risk Control Systems (IRCS)
- Helps determines organizational maturity level - according to best practices, against a clear set of external benchmarks
- RESULT – determines performance (strengths & weaknesses) around the 5 components and 17 principles of the (COSO IRCS Framework).

Why Maturity Assessments are Important

- Identifies business critical information to best allocate limited resources and facilitate effective business decision making
- Creates a base line to develop (next steps) to a “future state” that includes a higher level of strategic organizational maturity
- Identifies business opportunities for enhanced growth
- Helps articulate business capabilities and needs to different levels in the organization

IRCS Maturity Level Scale

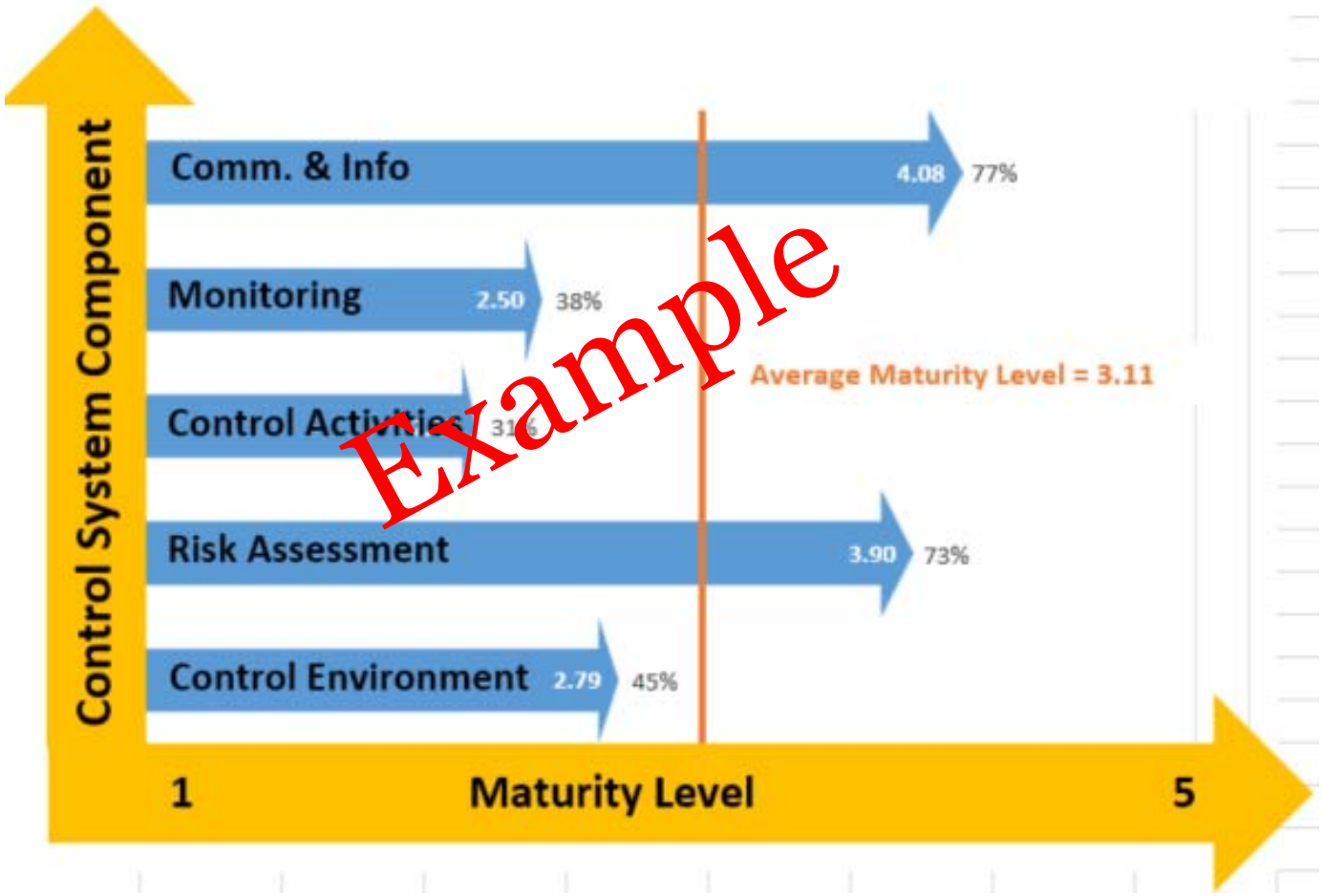


Maturity Assessment Process Steps

Utilizing COSO's Framework:

1. Identify who to include in the assessment (three levels)
2. Perform the assessment
3. Report the results
4. Analyze results and develop roadmap
5. Gain business alignment
6. Deploy results (staged results – does not happen overnight)

Maturity Level Results



Maturity Level Assessment Tool
(Example Component)

Q#	Assessment Factor	Guidance Questions	Indicator of Strong Controls	Indication of Weaker Controls	Assessment	Summary
					(Weak) 1 - 5	
		Section 1 – Control Environment				**2.79**
1	**Demonstrates Commitment to Integrity and Ethical Values**					**3.5**
1.1	Tone at the Top.	Does the oversight body and management demonstrate the importance of integrity and values through their directives, attitudes, and behavior?	The oversight body and management layers lead by example and demonstrate the importance of integrity and values. Tone is a driver or barrier to internal control. Core values are posted, and readily available for all staff.	The oversight body and management layers fail to lead by example or poorly demonstrates the importance of integrity and values. Tone is a barrier to internal control. Core values are institutionalized.	2	
1.2	Standards of conduct.	Does management understand the organizations policies governing relationships with regulators, the electric industry, and the public at large?	Policies are well understood.	Policies are poorly understood.	4	
1.3	Conflicts of interests.	Does management understand the organizations policies regarding potential conflicts of interest?	Policies are well understood.	Policies are poorly understood.	3	
1.4	Integrity.	Does management demonstrate and regularly communicates high expectations regarding integrity and ethical values?	Management set a good example and communicates high expectations regarding integrity and ethical values.	Management does not set a good example and/or does not communicate high expectations regarding integrity and ethical values.	5	
2	**Demonstrates Commitment to Competence**					**2.8**
2.1	Recruit and Retain talent	Does management demonstrate a commitment to recruit, develop, and retain competent individuals?	Strong, formal recruitment and retention strategy defined in organizational policy	Lack of formal recruitment and retention strategy, lack of development opportunities.	2	
2.2	Job descriptions.	Are responsibilities are clearly defined in writing and communicated as appropriate?	Compliance and Control Responsibilities are defined and communicated.	Compliance and Control Responsibilities are poorly defined or poorly communicated.		
2.3	Knowledge and Skills.	Does management understand the knowledge and skills required to accomplishorganization objectives?	Management adequately considers knowledge and skill requirements.	Management does not adequately consider knowledge and skill requirements.	4	
2.4	Employee competence.	Is management aware of competency levels and is involved in training and increased supervision when competency is low?	Management is adequately aware of competency levels and actively addresses problems.	Management is not adequately aware of competency levels and does not actively address problems.	3	
2.5	Staffing of critical functions.	Are critical functions adequately staffed, with reasonable workloads?	There is adequate staffing	There is inadequate staffing and frequent periods of overwork and "organizational stress."	1	
2.6	Turnover. Particularly turnover in positions with accountability to Controls	Is turnover functional or Dysfunctional? Does management understand root causes of turnover?	Low turnover rate. Management differenciates between functional and dysfunction turnover. Addresses root causes of dysfunctional turnover.	Dysfunctional turnover. Management does not understand root causes.	4	
3	**Management's Philosophy and Operating Style**					**1.60**
3.1	Risk Based Philosophy	Does management inspire a risk base philosophy and design a risk based approach with strong controls?	Management is directly responsible for the design, implementation, and operating effectiveness of an entity's internal control system. Company has an inventory of current compliance risks and control practices.	Lack of control systems in place - management expects lower level staff to design, implement, and operate the effectiveness of an entity's internal control system	3	
3.2	Communication with Regulators, industry and customers?	Does management insists on transparency with regulators, industry and customers?	Transparency is of part of the organizations approach to building business trust.	Management is secretive and reluctant to conduct business or deal with issues in an open manner.	1	
3.3	Laws and regulations.	Is there active management concern and effort to ensure compliance with the letter and intent of laws and regulations? When misconduct occurs, is it a repeat of the same offense or misconduct of a different nature?	Management activly engages to ensure laws and regulations are followed to letter and intent of laws and regulations.	Management is willing to risk the consequences of noncompliance.	1	
3.4	Exceptions to policy.	Exceptions to policy are infrequent. When they occur they must be approved and well documented.	All exceptions to policy must be reviewed, accepted and documented by management.	Exceptions to policy are the norm and are rarely documented.	2	
3.5	Violations of Regulations	How has the company responded to prior violations to Regulations? Did it take disciplinary action against employees involved in violations? When misconduct occurs, is it a repeat of the same offense or misconduct of a different nature?	All prior violations are captured, mitigated, tracked and used as lessons learned. Management is accountable for Control enviroment, risk assessment and communication elements of the control system. Owners of control activites are accountable for preventing reoccurance of control failures.	There is a lack of accountability on the accountability structure, re-ocurance of violations is common place.	1	

DEMO LINK

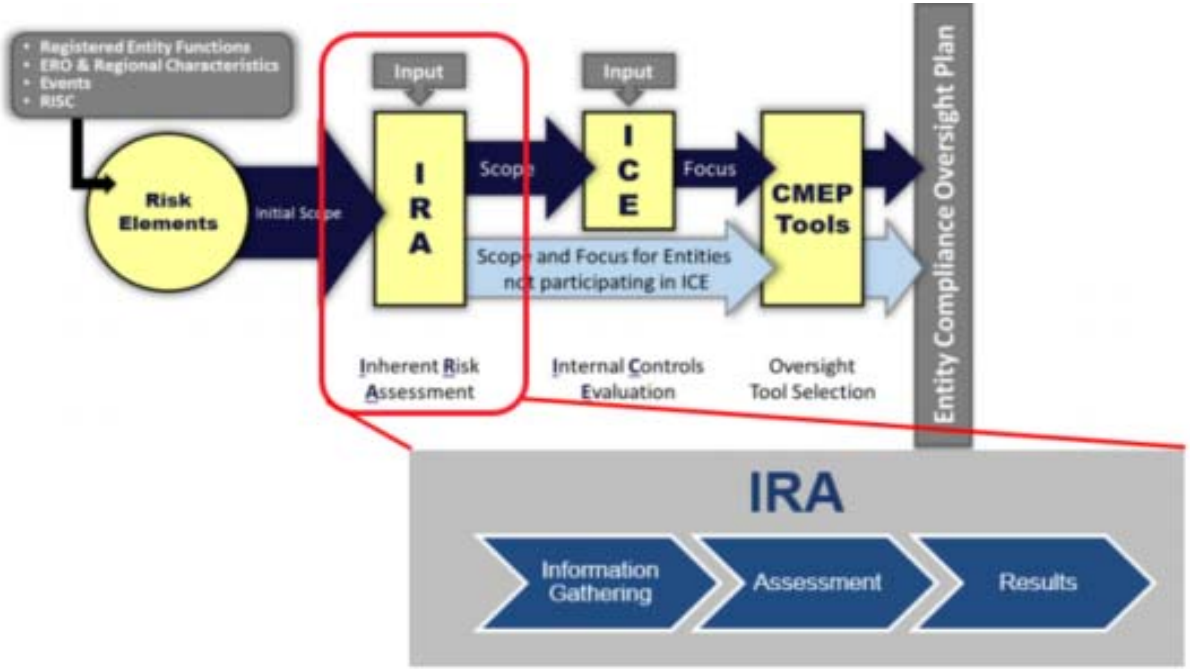
Inherent Risk Assessment

- A method to measure and articulate the level of inherent risk to the BES given an organization's functional registrations, capability, materiality, system design, configuration, size, location, past performance etc.

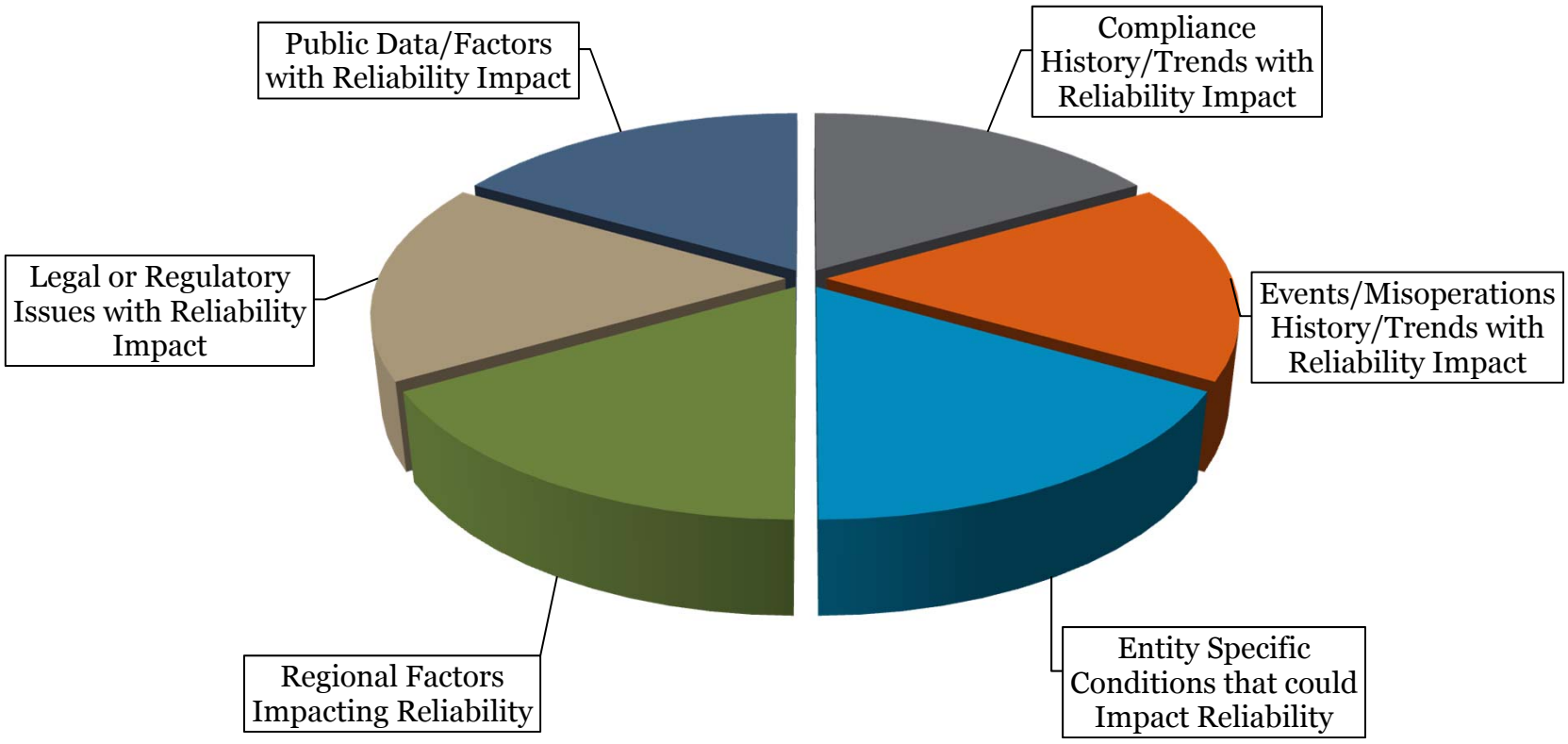
- RESULT - Establishes a qualitative and quantitative inventory of inherent risk factors posed by an individual registered entity to the reliability of the BES

IRA Tool

- GridSME's IRA Tool is designed around NERC's criteria for evaluating an entity's risk to the Bulk Electric System (BES)



Example Risk Assessments Factors



Inherent Risk Assessment Tool

Risk Factor	Risk Factor Subcategory	Low Risk Example	Moderate Risk Example	High Risk Example	Risk Level
System Geography	Geography	Entity has no areas of challenging system geography (rugged terrain, mountains, oceans, etc.)	Entity has a moderate amount of rugged terrain that impacts a moderate load of generation	Entity has a large amount of rugged terrain that impacts a large part of the bulk electric system	low
	Vegetation Management	Entity operates in a climate with low vegetation management issues	Entity operates in a climate with moderate vegetation management issues	Entity operates in a climate with extremely invasive vegetation and has faced issues affecting vegetation management in the	moderate
Peak Load and Capacity	Number of customers/NEL/critical customers	Entity provides service for less than 2% of the total region and no critical customers identified within the service area	Entity provides primary power supply for 10% - 20% of region	Entity provides primary power supply for 50%+ of region and/or provides power supply to major military bases, communication hubs, etc.	high
	Transmission Substation Voltage	No transmission	100kV-345kV	500KV+	high
	Total megawatt output (Generation)	<1000MW	1000MW - 5000MW	10000MW+	high
	Peak Load	<1000MW	1000MW - 5000MW	10000MW+	high

Esitmated Inhernet Risk: moderate

DEMO LINK

IRCS Reliability Standard Assessment

A method to measure and articulate the levels of risk and compliance readiness in relation to control activities that address the NERC Reliability Standards.

1. Effectively catalogs and documents all levels of internal controls

2. Evaluates and tests the design and operational performance (strengths & weaknesses) of the control activity component of the COSO IRCS Framework

3. Deficiency identification mechanism, assesses the reason for the deficiency and the related risk to help determine the appropriate level of correction (if one is required)

4. RESULT - defines the residual risk factor and control elements that are under or over controlled

Why IRCS Assessments are Important

- Catalogs and documents controls to better articulate control system health to regulators.
- Brings clarity to control design and operation (individually and in combination with other controls) to better determine capability of achieving objectives and address related risks
- Identifies business critical information to best allocate limited resources and facilitate effective business decision making
- Determines if controls are effectively and dynamically monitored for competence

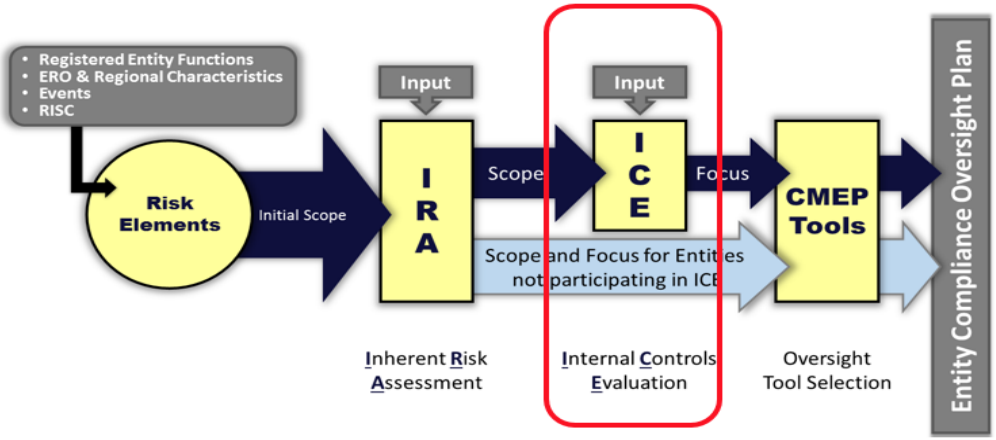
IRCS Reliability Standard Assessment Tool

GridSME SUBJECT MATTER EXPERTS

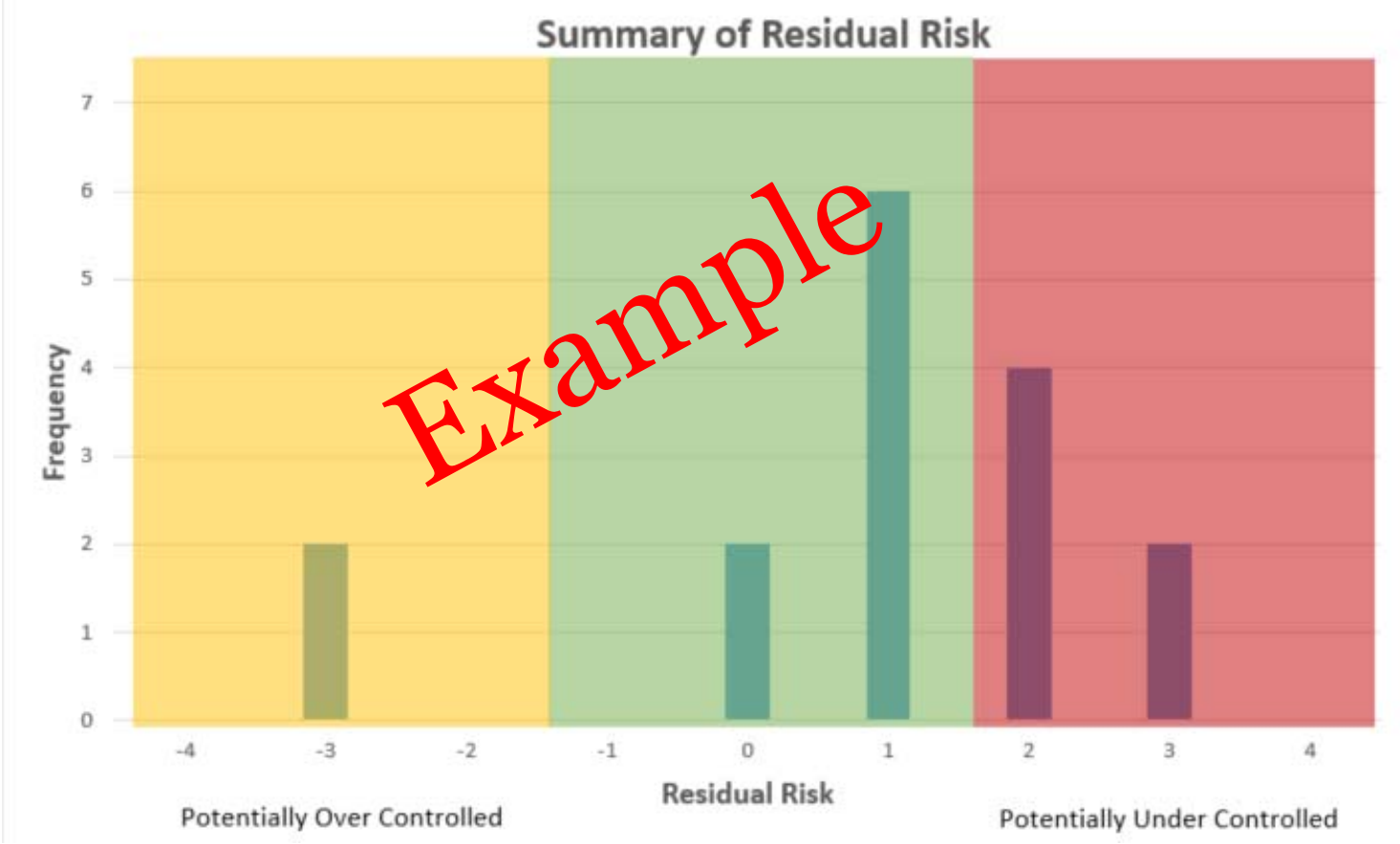
IRCS Reliability Standard Assessment

Client		Project		Audit Date		Contact Name		Contact #	

Interviewer	Interviewee	Select All Applicable Registered Functions and Click Finish (One time set up)							
		BA	DP	GO	GOP	IA	LSE	PA	Finish
		PC	PSE	RC	RP	RRO	RSG	TO	
		TOP	TP	TSP	CIP Low	CIP Med	CIP High		



IRCS Control Attribute Assessment Results



IRCS Control Attribute Assessment
(Roll-Up)

Reliability Standard	Requirement	Text of Standard	Violation Risk Factor (VRF)	Inherent Risk Factor	Risk Element	Primary Control?	Secondary Control?	Tertiary Control?	Residual Risk Factor	Complimentary?	Frequency Appropriate for Risk and Control Type?	Auto/Man Matches Frequency?
CIP-006-5	2.1.	Require continuous escorted access of visitors (individuals who are pro vided access but are not authorized for unescorted physical access) wit hin each Physical Security Perimeter, except during CIP Exceptional Circ umstances.	Medium	2.835	physical security	yes	yes	yes	0.17	complimentary	yes	investigate primary
CIP-006-5	2.2.	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual po int of contact responsible for the visitor, except during CIP Exceptional Circumstances	Medium	2.835	physical security	yes	yes	yes	0.17	not complimentary	investigate secondary	yes
CIP-006-5	2.3.	Retain visitor logs for at least ninety calendar days.	Medium	2.835	physical security	yes	no	no	2.00	N/A	yes	investigate primary
CIP-006-5	R3.	Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) th collectively include each of the applicable requirement parts in CIP-006-5 Table R3 – Maintenance and Testing Program.	Lower	1.4175	physical security	yes	yes	yes	-2.75	not complimentary	investigate primary	investigate tertiary
CIP-006-5	3.1.	Maintenance and testing of each Physical Access Control System and lo cally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	Lower	1.4175	physical security	yes	yes	yes	-2.75	not complimentary	yes	yes
CIP-007-5	1.1	Where technically feasible, enable only logical network accessible port s that have been determined to be needed by the Responsible Entity, incl uding port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on th e device then those ports that are open are deemed needed.	Medium	2.835	cyber security	yes	no	no	1.50	N/A	yes	yes
CIP-007-5	1.2	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	Medium	2.835	cyber security	yes	no	no	1.50	N/A	yes	investigate primary
CIP-007-5	2.1	A patch management process for tracking, evaluating, and installing cy ber security patches for applicable Cyber Assets. The tracking portion s hall include the identification of a source or sources that the Responsib le Entity tracks for the release of cyber security patches for applicable C yber Assets that are updateable and for which a patching source exists.	Medium	2.835	cyber security	yes	no	no	1.50	N/A	yes	yes

DEMO LINK

Return on Investment

- Improved operating efficiency
- Improved grid reliability
- Increased compliance certainty
- Reduce human drift
- Reduce Latent Organizational Deficiencies
- Reduce organizational risk
- Reduce audit preparation resource hours
- Reduce/eliminate violations and penalties
- Smaller Compliance engagements
- Reliability and integrity of critical information
- Safeguarding of assets
- Cost savings, Profit and Growth

Questions

- How Mature is your organization reside on the Internal Risk Control Maturity Scale?
- Can you currently define the residual risk factors and control elements that are under or over controlled?
- What Tools does your organizations use to catalog controls in order to articulate control system health?
- What challenges or barriers does your organization have in implementing an Internal Risk Control System?

References

- Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control - Integrated Framework, 2013 version
- The Institute of Internal Auditors – International Professional Practices Framework – Standard 2210 – Engagement Objectives
- Standards for Internal Control in the Federal Government, GAO, Sep 2014
- United States Government Accounting Office - Government Auditing Standards – Chapter 7 – Reporting Standards for Performance Audits
- American Institute of Certified Public Accountants – Professional Standards, vol. 1 – AU Section 314
- ERO Enterprise Internal Control Evaluation Guide, Oct 2014
- ERO Enterprise Inherent Risk Assessment Guide, Oct 2014
- PwC *Risk in Review* survey of 1,229 senior executives and board members. ***Risk in review*** Decoding uncertainty, delivering value, April 2015

Self Scouting

Crisis defines a company - an organization's reputation hinges on its weakest vulnerabilities

- Risk Based Thinking
- Find and Fix Mentality
- Gap Analysis

- Defines the vulnerabilities and lynch Pins, identifies the breakpoints