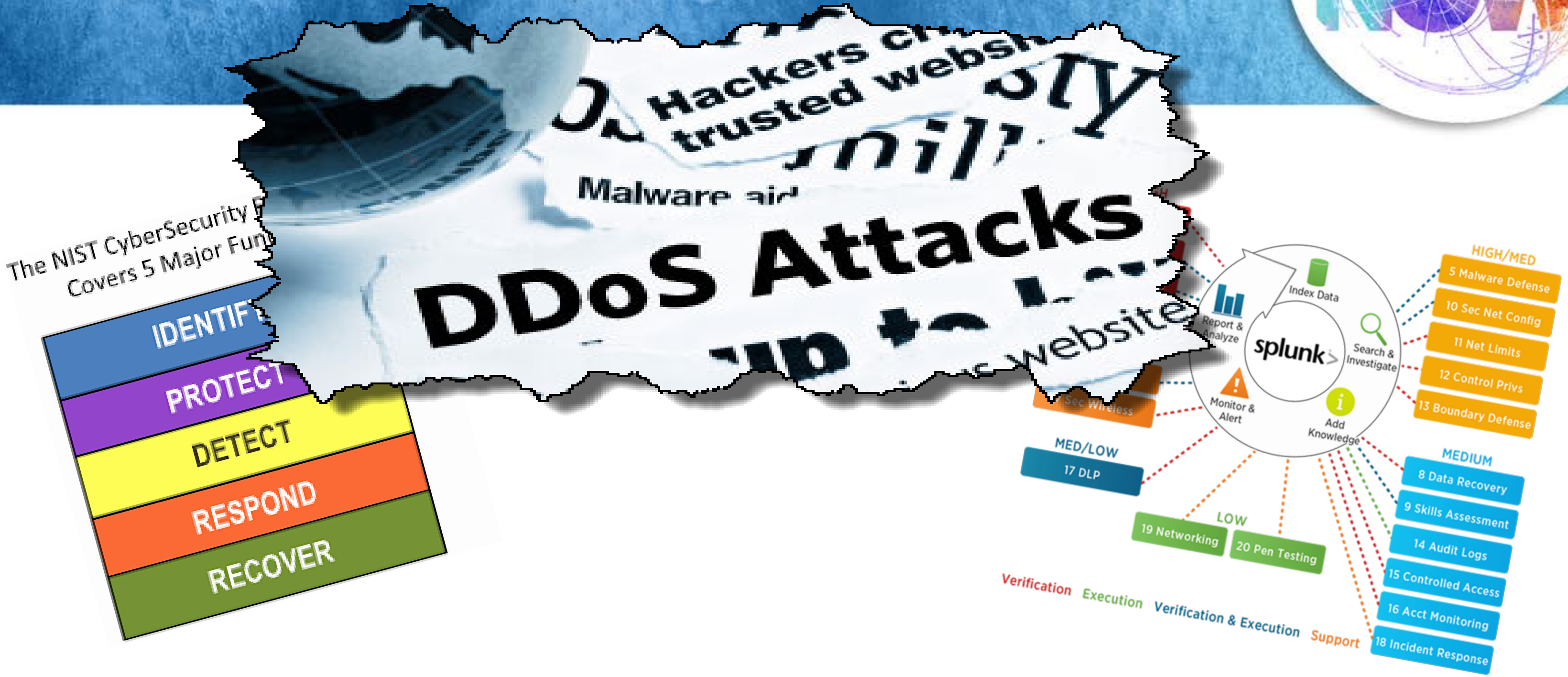
RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: GRC-W02

# THERE'S NO SUCH THING AS A CYBER-RISK

**Evan Wheeler**

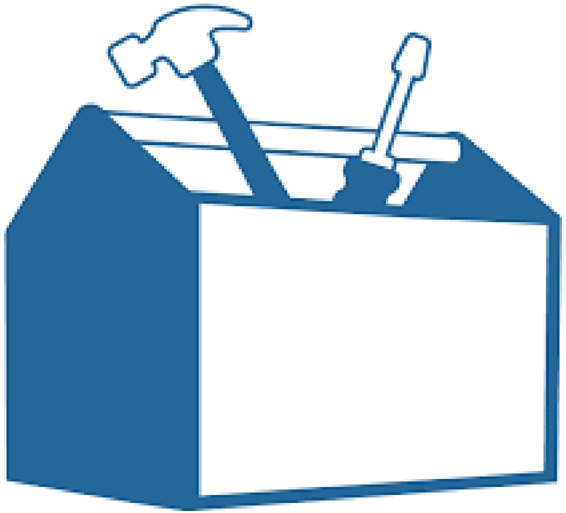
CISO, VP Risk Management
Financial Engines



## Your boss asks you to identify the top information risks for your organization …

where do you start?

# Tools of the Trade @ERM



- Inherent Risk Profile
- Loss Event Analysis
- Scenario Analysis
- RCSA
- PRC Library
- Control Testing

# PUTTING RISK INTO CONTEXT

# Are these our top risks?

Mobile Devices

Cloud Computing

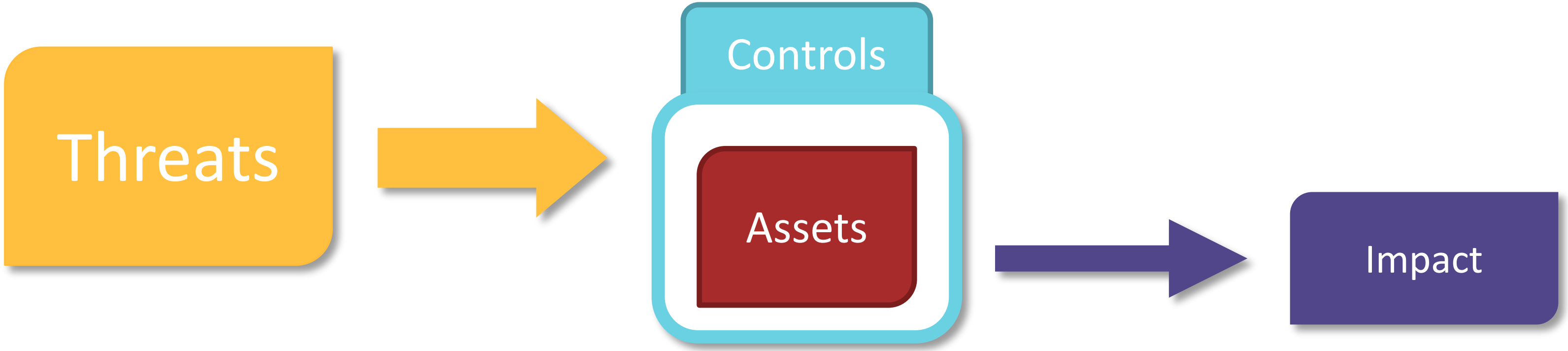
Insiders

Credential Theft

Supply Chain

# Definition of Cyber Risk

The potential that **threats** will successfully exploit vulnerabilities of an **asset** and cause harm



Articulating a risk:

- Implies some degree of uncertainty
- Must describe a potential outcome

# Us & Them (ERM)

- Macroeconomic
- Strategic
- Operational

- ❑ Regulatory change & scrutiny
- ❑ Compliance
- ❑ Fraud
- ❑ Safety
- ❑ Business Continuity
- ❑ Economic Conditions
- ❑ Geopolitical
- ❑ Conduct
- ❑ Resistance to Change
- ❑ Succession & Talent
- ❑ IT Failure
- ❑ Disruptive innovations
- ❑ Cyber Attacks

# Business Outcomes

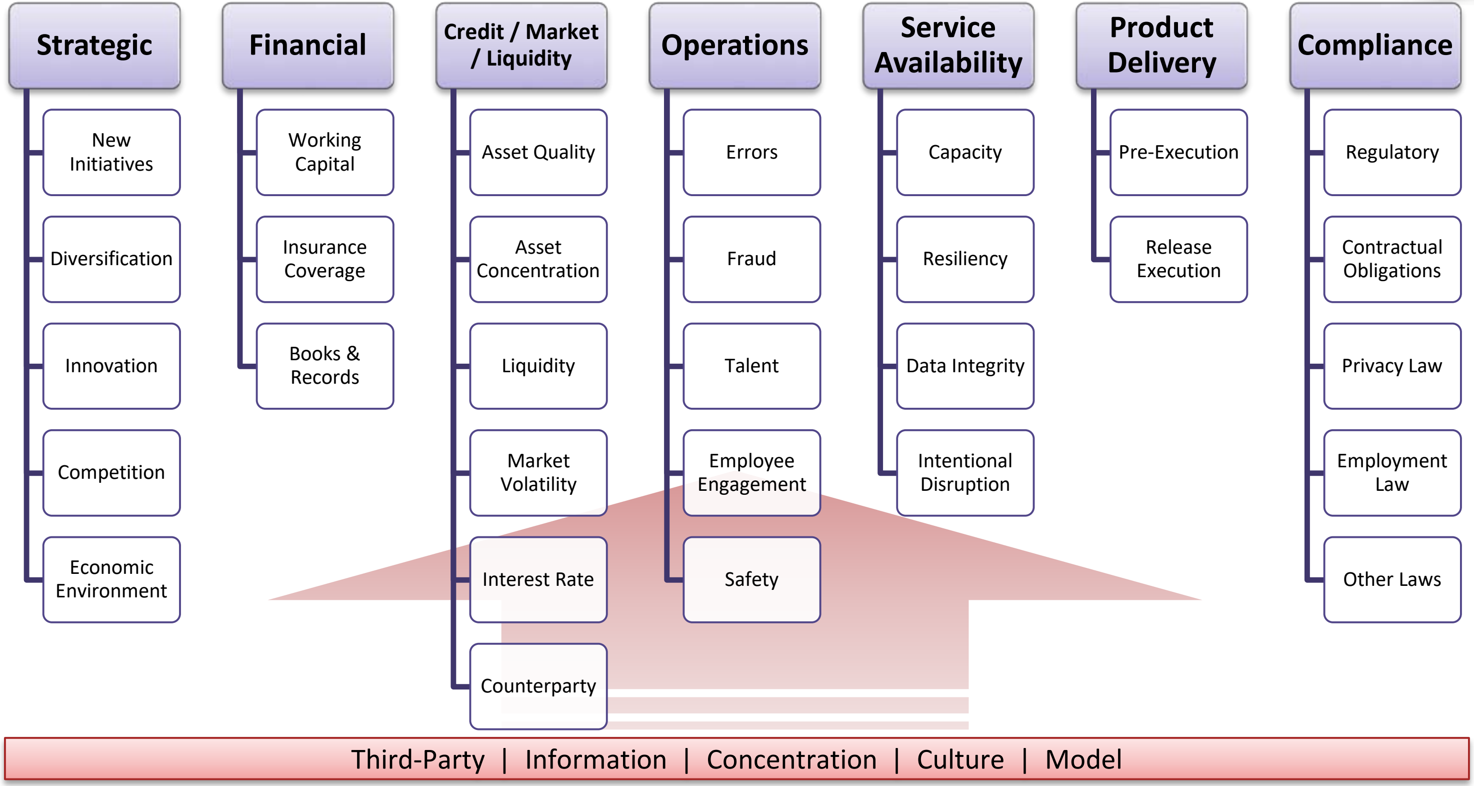
**Examples**

- Losing a strategic client or partner
- Regulatory sanctions
- Compressed profit margins
- Expensive lawsuits
- Damage to brand
- Loss of life

# Risk Examples @ERM

| Category | Risk Description |
|---|---|
| **Regulation** | Regulatory non-compliance may result in a fine, business loss, or increased cost of compliance |
| **Outsourcing** | Regulator may find that third-party oversight controls are deficient resulting in fines from regulators and negative publicity |
| **AML, CTF and sanctions compliance** | Malicious actors may conduct transactions through our services to facilitate illegal or sanctioned activities resulting in resource intensive investigations, fines and settlement costs |
| **Fraud** | Malicious actors (external or internal) may defraud the organization or clients resulting in direct financial loss, costly investigations, and penalties or lawsuits. |

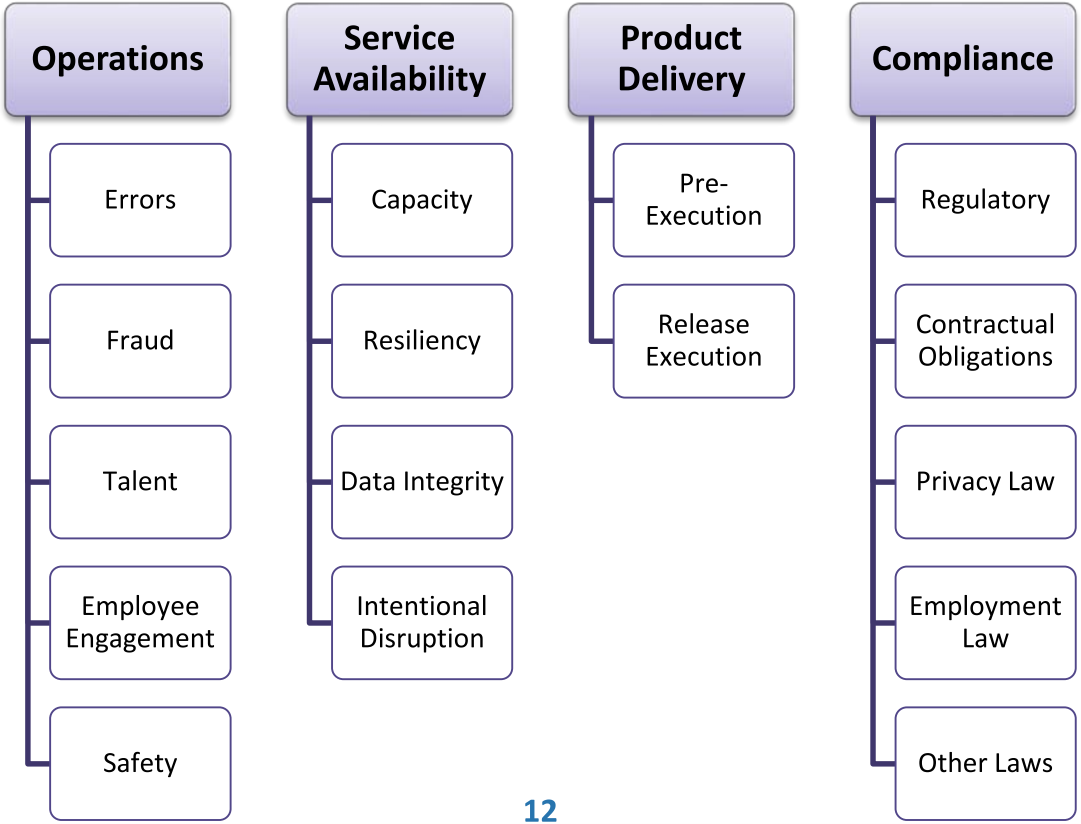
# Risk Universe



| Strategic | Financial | Credit / Market / Liquidity | Operations | Service Availability | Product Delivery | Compliance |
|---|---|---|---|---|---|---|
| New Initiatives | Working Capital | Asset Quality | Errors | Capacity | Pre-Execution | Regulatory |
| Diversification | Insurance Coverage | Asset Concentration | Fraud | Resiliency | Release Execution | Contractual Obligations |
| Innovation | Books & Records | Liquidity | Talent | Data Integrity | | Privacy Law |
| Competition | | Market Volatility | Employee Engagement | Intentional Disruption | | Employment Law |
| Economic Environment | | Interest Rate | Safety | | | Other Laws |
| | | Counterparty | | | | |

Third-Party | Information | Concentration | Culture | Model

# Operational Risk Domains



**Operations**
- Errors
- Fraud
- Talent
- Employee Engagement
- Safety

**Service Availability**
- Capacity
- Resiliency
- Data Integrity
- Intentional Disruption

**Product Delivery**
- Pre-Execution
- Release Execution

**Compliance**
- Regulatory
- Contractual Obligations
- Privacy Law
- Employment Law
- Other Laws

# LOSS EVENT ANALYSIS

# Risk vs. Incident

- When you evaluate a ***risk***, you are estimating the future potential for some event(s).  It will have ranges of probable impact and likelihood of occurrence (or frequency of re-occurrence).

- When you evaluate an ***incident***, that is a point in time impact assessment.  It may or may not have a measurable impact, and when active may have varying degrees of urgency to resolve.

# Forms of Loss* (Magnitude)

**Productivity**

Operational inability to deliver products or services resulting in unrealized revenue (i.e. $ / time)

**Response**

Costs of managing an event (i.e. communication, regulatory demands, etc.)

**Replacement**

Replacement of capital assets (i.e. applications, personnel, etc.)

**Fines & Judgments**

Fines or judgments levied against the organization through civil, criminal or contractual actions

**Reputation / Competitive Adv.**

External stakeholder perspective on organization's value decreased or liability increased, or intellectual property or key competitive differentiators damaged

* These categories of loss and definitions are extracted from the Factor Analysis of Information Risk (FAIR) methodology.

# Pre-Defined Loss Tables - Sample

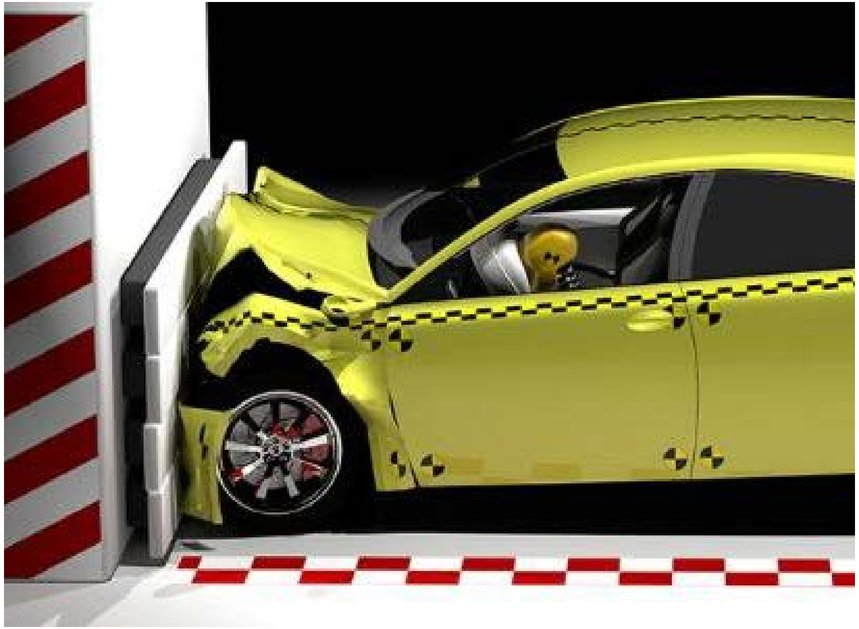
| Magnitude | Min | Max | Productivity[1] | Response[2] | Replacement |
|---|---|---|---|---|---|
| **Severe** | $25m | Above | Full service exceeds 1 business day, or degradation exceeds 1 week | 1,000 hours or more | Funding approval from Board required |
| **High** | $1m | <$25m | Full service exceeds RTO, or partial exceeds RTOx2 | 500 up to 1,000 hours | Requires out of budget funding |
| **Moderate** | $500k | <$1m | Partial service up to RTOx2, or full service up to RTO | 100 up to 500 hours | In function's budget but postpones planned investment |
| **Low** | $5k | <$500k | Partial service up to RTO | 5 up to 100 hours | Replacement cost in function's discretionary budget |
| **Immaterial** | $0 | <$5k | No SLA breach | up to 5 hours | No cost or covered by insurance |

1. Assumes revenue isn't collected during downtime and won't be recuperated afterwards
2. Avg. loaded person hourly rate @ $75 - $150

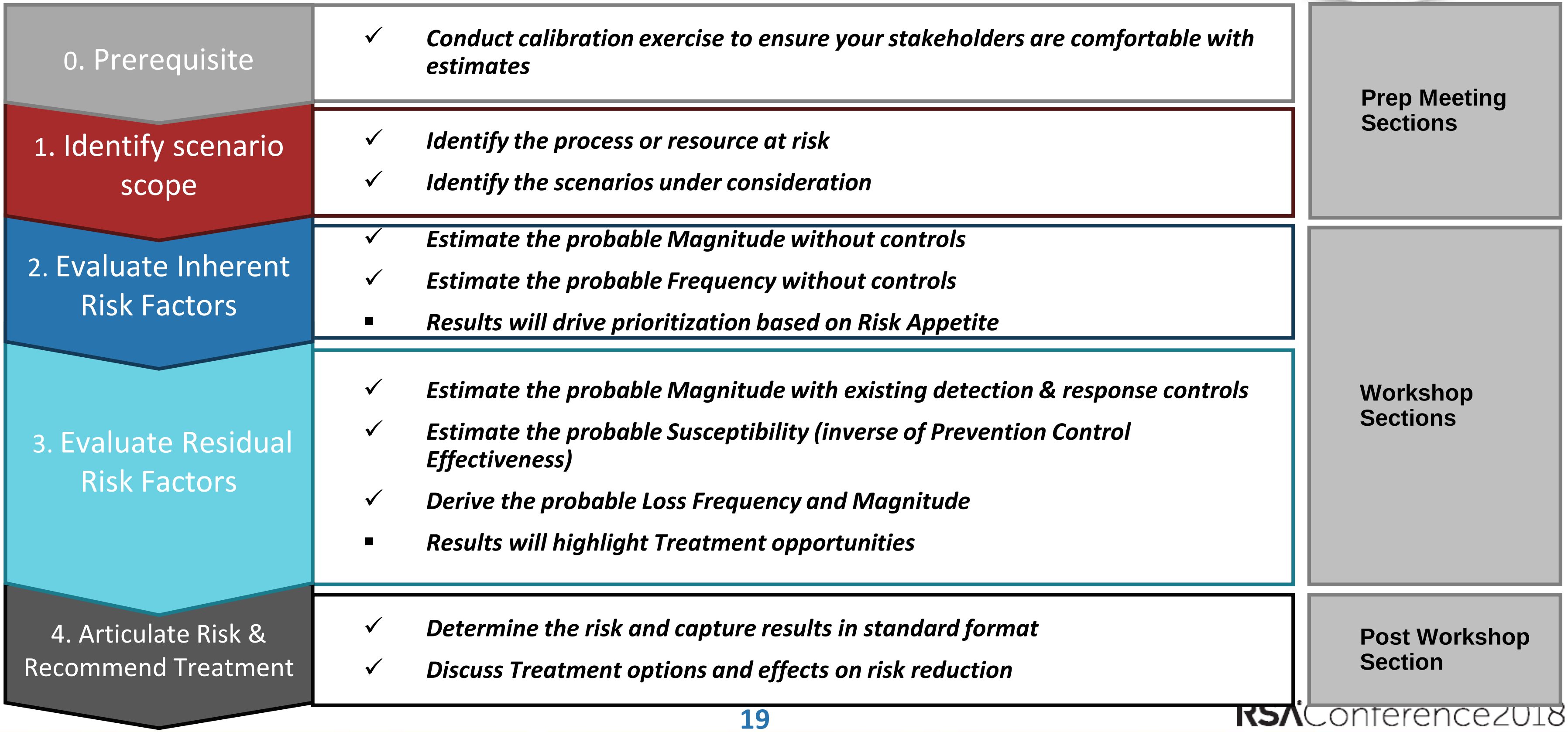
# SCENARIO ANALYSIS

# Let’s run a scenario …

**ERM** vs. **Cyber**



# Workshop Style Scenario Analysis



| | | |
|---|---|---|
| 0. Prerequisite | ✓ *Conduct calibration exercise to ensure your stakeholders are comfortable with estimates* | Prep Meeting Sections |
| 1. Identify scenario scope | ✓ *Identify the process or resource at risk*<br>✓ *Identify the scenarios under consideration* | |
| 2. Evaluate Inherent Risk Factors | ✓ *Estimate the probable Magnitude without controls*<br>✓ *Estimate the probable Frequency without controls*<br>▪ *Results will drive prioritization based on Risk Appetite* | Workshop Sections |
| 3. Evaluate Residual Risk Factors | ✓ *Estimate the probable Magnitude with existing detection & response controls*<br>✓ *Estimate the probable Susceptibility (inverse of Prevention Control Effectiveness)*<br>✓ *Derive the probable Loss Frequency and Magnitude*<br>▪ *Results will highlight Treatment opportunities* | |
| 4. Articulate Risk & Recommend Treatment | ✓ *Determine the risk and capture results in standard format*<br>✓ *Discuss Treatment options and effects on risk reduction* | Post Workshop Section |

# Scenario Analysis

| Loss Event Scenarios | Risk Domain |
|---|---|
| Product quality could suffer if QA time is compressed | |
| A nation state attacker could cause a prolonged disruption of a critical service with a blended DDoS attack | |
| Over time the company could become materially out of compliance with international privacy laws if changes aren’t sufficiently monitored | |
| Sales executive could leave the company and take client data to competitor | |
| A recently terminated employee could sabotage infrastructure if access isn’t removed timely | |

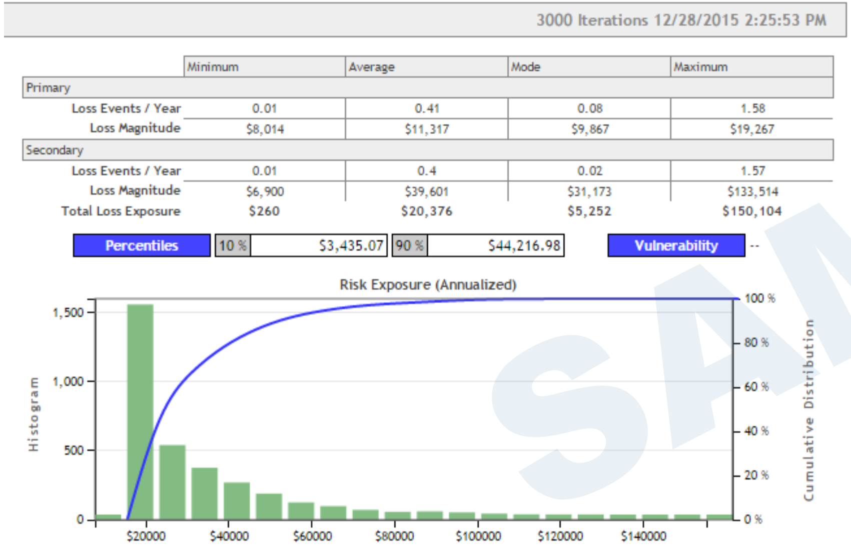
# Unrecoverable data from a ransomware attack

| | | | |
|---|---|---|---|
| **Asset at Risk** | ☑ Hospital X, Application Y<br>☑ Patient Medical Test Records | **Risk Ownership** | ▪ Business Unit Head |
| **Threat Community** | ☒ Amateur Hacker<br>☒ Privileged Insider<br>☒ Nation State<br>☑ Cyber Criminal | **Forms of Loss** | ☑ Productivity<br>☑ Response<br>☒ Replacement<br>☑ Fines & Judgments<br>☑ Reputation / Competitive Advantage |
| **Motivation** | ☒ Accidental<br>☑ Malicious | **Top Risk** | ▪ Service Availability<br>▪ Legal / Regulatory |
| **Impact Area** | ☒ Confidentiality<br>☒ Integrity<br>☑ Availability | **Key Controls** | ▪ Phishing campaigns<br>▪ Application whitelisting<br>▪ Data backups |

| | |
|---|---|
| **Assumptions** | ▪ Approximately 1,000 patient records in application<br>▪ Health records fall under HIPAA regulations<br>▪ Ransom won’t be paid<br>▪ Restoration of backup data is unreliable and often fails<br>▪ Not all impacted patients will notice an impact directly<br>▪ Patient turnover (loss of future business) would be minimal<br>▪ Insurance will cover some response costs<br>▪ Some records could be recreated from paper and manually re-entered |

# Sample Results

## Data Theft



3000 Iterations 12/28/2015 2:25:53 PM

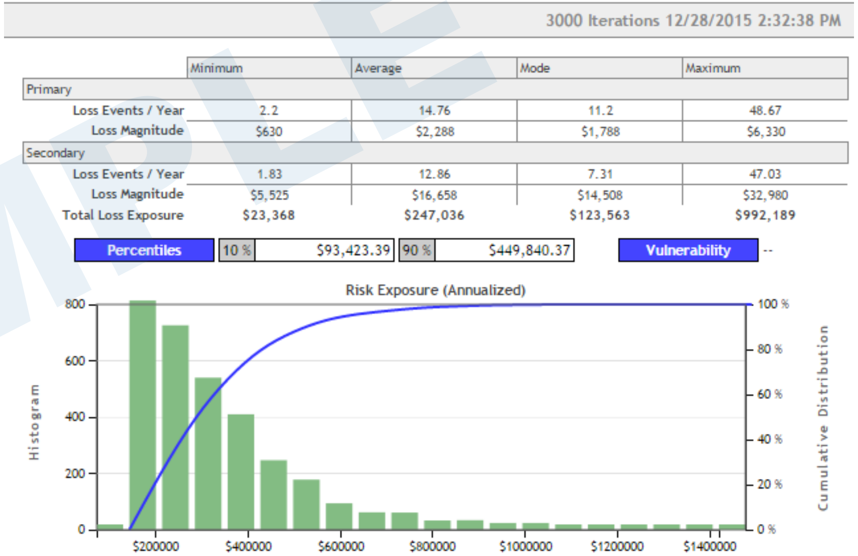
| | Minimum | Average | Mode | Maximum |
|---|---|---|---|---|
| Primary | | | | |
| Loss Events / Year | 0.01 | 0.41 | 0.08 | 1.58 |
| Loss Magnitude | $8,014 | $11,317 | $9,867 | $19,267 |
| Secondary | | | | |
| Loss Events / Year | 0.01 | 0.4 | 0.02 | 1.57 |
| Loss Magnitude | $6,900 | $39,601 | $31,173 | $133,514 |
| Total Loss Exposure | $260 | $20,376 | $5,252 | $150,104 |

| Percentiles | 10 % | $3,435.07 | 90 % | $44,216.98 | Vulnerability | -- |
|---|---|---|---|---|---|---|

**Single Loss Max: $150k**

**Annualized: $45k**

## Accidental Disclosure



3000 Iterations 12/28/2015 2:32:38 PM

| | Minimum | Average | Mode | Maximum |
|---|---|---|---|---|
| Primary | | | | |
| Loss Events / Year | 2.2 | 14.76 | 11.2 | 48.67 |
| Loss Magnitude | $630 | $2,288 | $1,788 | $6,330 |
| Secondary | | | | |
| Loss Events / Year | 1.83 | 12.86 | 7.31 | 47.03 |
| Loss Magnitude | $5,525 | $16,658 | $14,508 | $32,980 |
| Total Loss Exposure | $23,368 | $247,036 | $123,563 | $992,189 |

| Percentiles | 10 % | $93,423.39 | 90 % | $449,840.37 | Vulnerability | -- |
|---|---|---|---|---|---|---|

**Single Loss Max: $10k**

**Annualized: $450k**

# Insurance in Assessments

- List limits and sub-limits of the coverage including dollar limit
- Scope of coverage

**Example:**

- A disclosure of sensitive data could result in legal action or financial claims from clients for damages.
- Risks of an intentional act of sensitive data theft would most likely be covered under the Financial Institution Crime and Computer Crime policy - annual aggregate of $XXM.
- Risks of a disclosure caused by an unintentional operational failure would most likely fall into the Product Failure category of loss, which is covered under the Commercial General Liability policy  - $XXM/occurrence, $XXM Aggregate, Umbrella $XXM.
- Also requires $XXM in liability coverage for vendors.

# RCSA

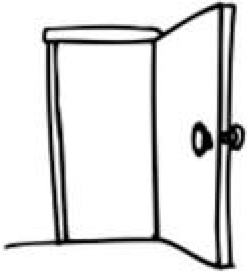
# Cyber | Risk

What are you protecting?

Who wants it?

- Motivation
- Capability
- Intent

How will they attack you?



Where are you vulnerable?

# Enterprise | Risk

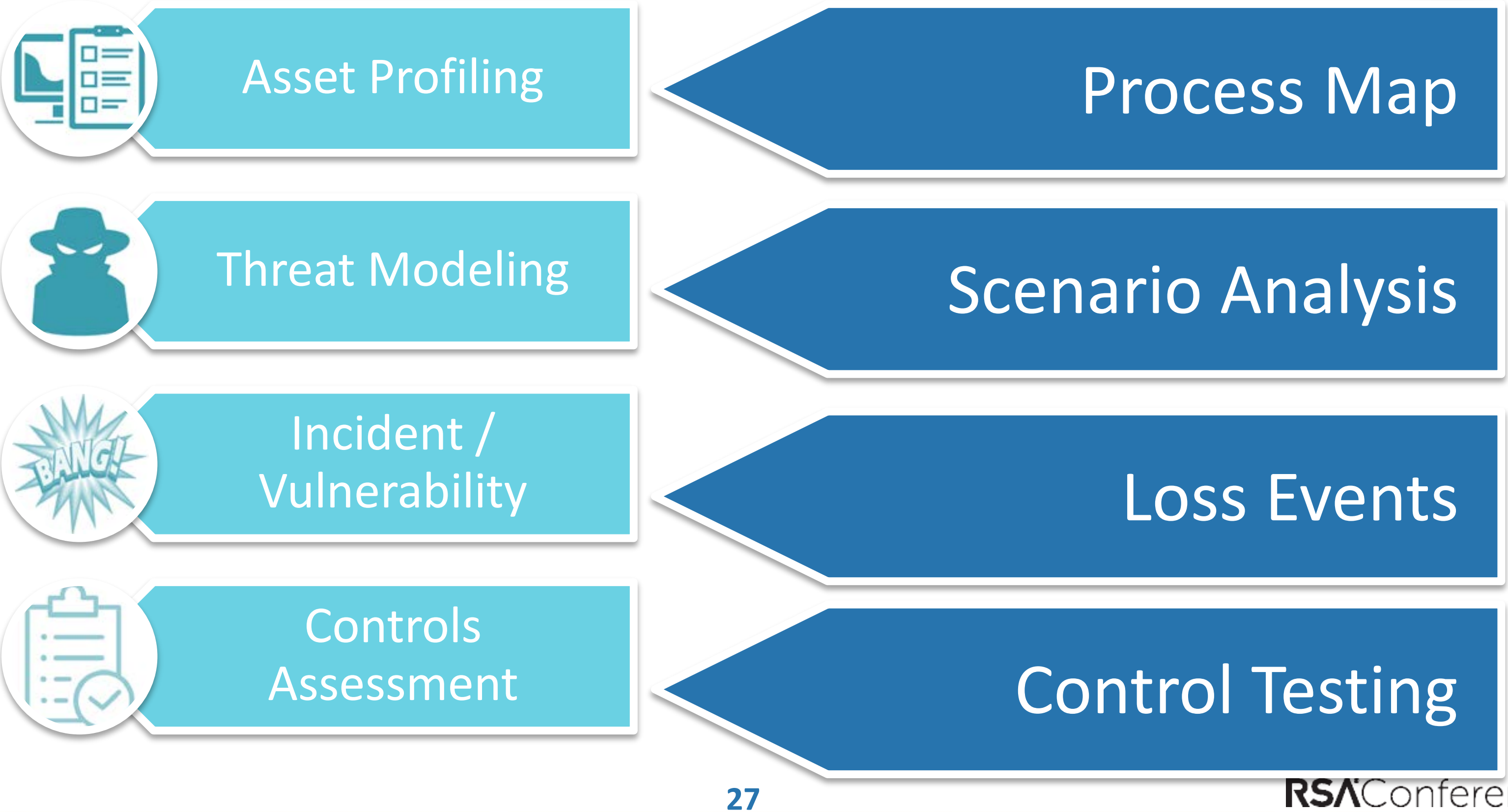
Inherent Risk

- Control Environment

Residual Risk

- Potential impact and likelihood sans controls
- Design and operating effectiveness of control environment
- Remaining risk exposure

# Where do you start assessing? @ERM



Asset Profiling

Process Map

Threat Modeling

Scenario Analysis

Incident / Vulnerability

Loss Events

Controls Assessment

Control Testing

# Risk & Control Self-Assessment (Top Down)

- Can be a self-assessment or facilitated
- Start with a baseline or library of controls
- Typically aligned to industry frameworks and regulatory requirements
- Ideally maps to the business processes, key risks, and the relevant controls

Process, Risk, and Control

Processes
Owners
Risks
Threat Scenarios
Control Objectives
Controls
Industry References

Library

# IT Processes - Sample

## Service Design

- Availability Management
- Capacity Management
- IT Service Continuity Management
- Service Level Management
- Security Management

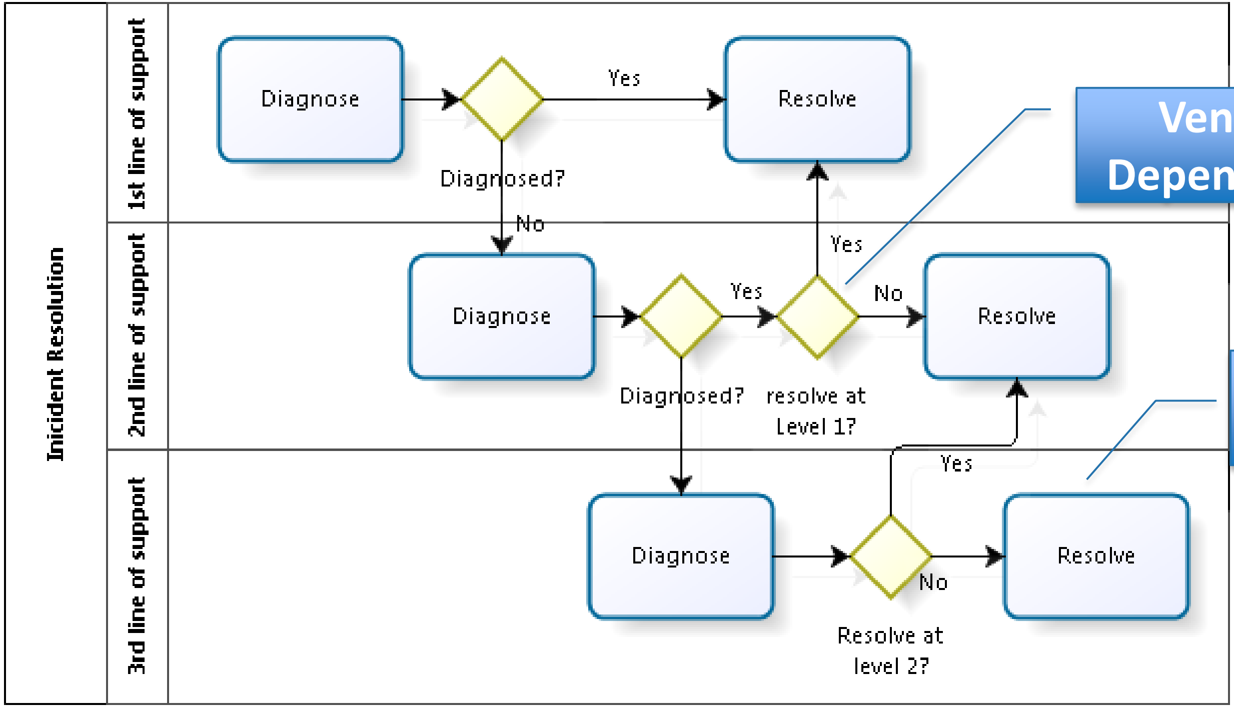
## Service Transition

- Asset Management
- Configuration Management
- Change Management
- Release Management

## Service Operation

- Service Desk
- Identity Management
- Job Scheduling
- Incident Management
- Problem Management

# Identify the business process flow, key control points, and dependencies



Vendor Dependency

Control Point

# Risks & Controls (IT Processes)

## Key Risks

1. Events may not be monitored, evaluated and escalated leading to potential service disruptions, or incidents may not be effectively identified and resolved leading to deviations from service level agreements.
2. Underlying cause may not be identified accurately resulting in work-around and/or permanent fixes inefficiently or ineffectively provided

## Key Controls

- Events are monitored and evaluated to determine the impact they may have on the delivery of services.
- Events that have been identified as having a potential to negatively impact the delivery of services are escalated and turned into incidents.
- Incidents and issues are documented and appropriately classified upon being reported.
- Problems are appropriately identified, classified and recorded.
- Problems are tracked to determine status (i.e. closed, problem abandonments, root cause, known error or correction failed).
- Problems are investigated and diagnosed to identify and record root cause.

# Risks & Controls (Business Processes)

## Key Risks

**Product Delivery** - The risk that the organization will not develop and deliver products and services in a timely manner and with the necessary functionality to meet the expectations of our clients and the marketplace.

**Service Availability -**
The risk that a financial or reputational loss will be incurred as a result of the inability to provide a required or expected level of service availability to clients.

**Legal & Regulatory Compliance** - The risk that a financial or reputational loss will be incurred as a result of a violation of law or regulation or as a result of the inability to enforce or adhere to contractual agreements.

## Key Controls

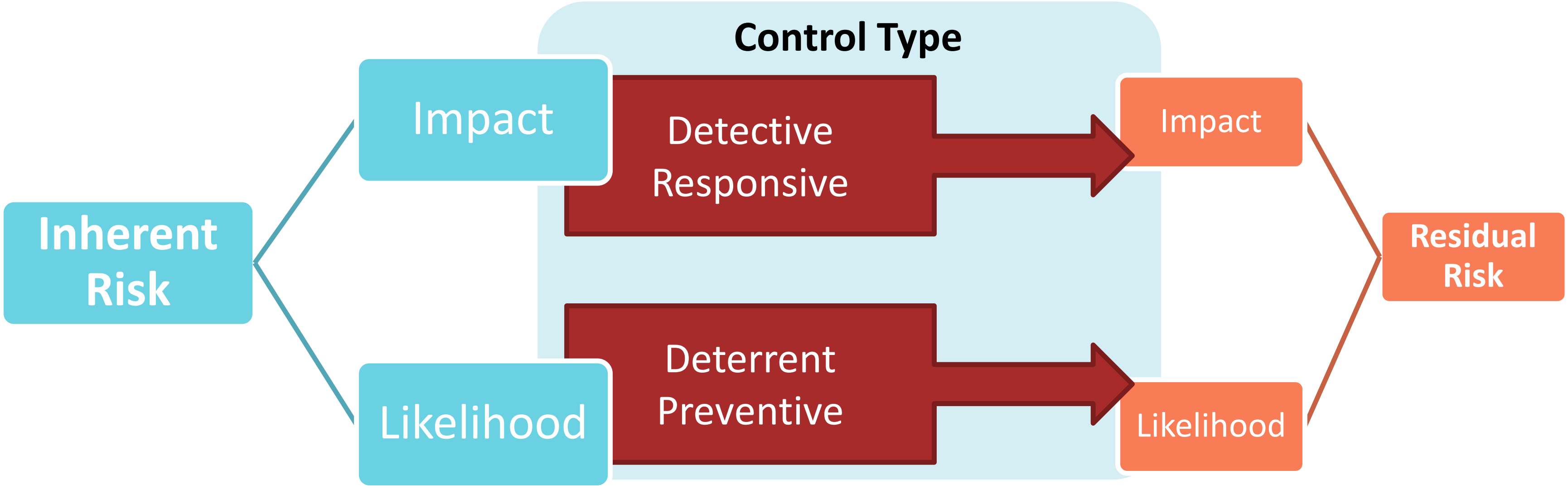
- SLAs
- Continuity Plans
- Change Management Approvals
- Access Recertifications
- Compliance Training

# Evaluating Controls – Sampling

| Control Rating | Criteria | Probability of Threat Success |
|---|---|---|
| **Strong** | ▪ Control is assessed to be designed and performed adequately, addresses control objectives, and mitigates the associated risk<br>▪ Testing of the control does not identify testing exceptions and indicates control is operating as intended<br>▪ Control is appropriately documented<br>▪ **Effective even under stress conditions** | 20% - 0% |
| **Average** | ▪ Control is assessed to partially mitigate risks, but not to be fully effective in how it is designed and/or performed<br>▪ Testing of the control identifies ad hoc testing exceptions and indicates that the control is not consistently operating as intended<br>▪ Control is not formally documented<br>▪ **Effective during normal conditions, but fails under stress conditions** | 50% - 20% |
| **Weak** | ▪ Control is assessed to not be designed or performed adequately and requires significant improvement in order to address control objectives<br>▪ Testing of the control identifies systematic testing exceptions and indicates the control is not operating as intended<br>▪ The control environment is not formally documented<br>▪ **Regular control failures are observed under normal conditions** | 80% - 50% |
| **Ineffective or Not Implemented** | ▪ Either control doesn't exist, or is only observed to only occasionally be effective by luck | 100% - 80% |

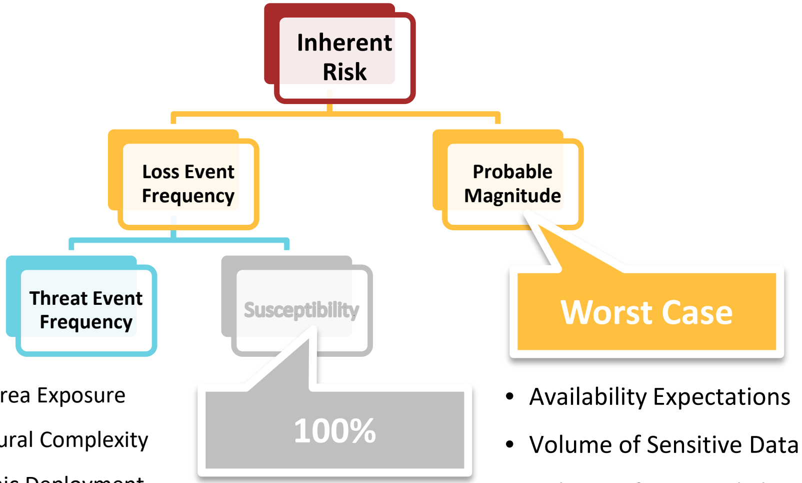
# BOTTOM UP RISK

# Controls



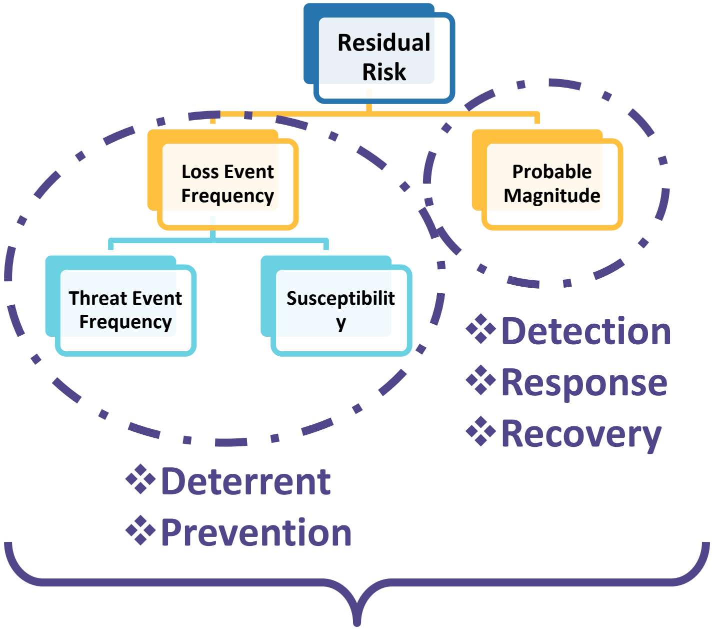
Control Type
Inherent Risk
Impact
Likelihood
Detective Responsive
Deterrent Preventive
Impact
Likelihood
Residual Risk

# Adapting FAIR for Inherent Risk



- Surface Area Exposure
- Architectural Complexity
- Geographic Deployment
- Geographic Usage
- Velocity of Change

- Availability Expectations
- Volume of Sensitive Data
- Volume of Financial Throughput
- Legal and Regulatory Impact
- Customer and Reputational Impact



Control Effectiveness

- Impact is estimated as worst case scenario
- Susceptibility to threats is considered 100%, essentially ignoring preventative controls

# Response Cost

| Magnitude | Min | Max | Data Classification | Records |
|---|---|---|---|---|
| Severe | $25m | Above | Confidential | B2B: ≥1,000<br>B2C: ≥1,000,000 |
| High | $1m | <$25m | Confidential | B2B: ≥100 <1,000<br>B2C: ≥10,000 <1,000,000 |
| Moderate | $500k | <$1m | Confidential | B2B: <100<br>B2C: <10,000 |
| Low | $5k | <$500k | Internal Use Only | |
| Immaterial | $0 | <$5k | Public | |

**Credit Monitoring Cost**

| Range of Records | Min | M/L | Max |
|---|---|---|---|
| 1 - 9 | - | - | $25 |
| 10 - 99 | - | $36 | $200 |
| 100 - 999 | $10 | $306 | $2,000 |
| 10,000 - 999,999 | $1,000 | $29,700 | $200,000 |

Additional Costs can include:

- Investigation
- Notification
- Customer Support
- Meetings
- Legal Counsel
- Public Relations

**Business to Business (B2B)** – represents institutional or corporate customer data that wouldn't fall under personal data definitions. Protection of this data is generally covered in contracts rather than laws.

**Business to Consumer (B2C)** – represents customer data for individuals.

# Productivity Loss

| Magnitude | Min | Max | Service Disruption[1] |
|---|---|---|---|
| **Severe** | $25m | Above | Full service exceeds 1 business day, or degradation exceeds 1 week |
| **High** | $1m | <$25m | Full service exceeds RTO, or partial exceeds RTOx2 |
| **Moderate** | $500k | <$1m | Partial service up to RTOx2, or full service up to RTO |
| **Low** | $5k | <$500k | Partial service up to RTO |
| **Immaterial** | $0 | <$5k | No SLA breach |

| Contingency Tier[2] |
|---|
| Tier 0<br>RTO = 0 – 1 hours |
| Tier 1<br>RTO = 1 – 4 hours |
| Tier 2<br>RTO = 4 – 12 hours |
| Tier 3<br>RTO = 12 – 24 hours |
| Tier 4<br>RTO = > 24 hours |

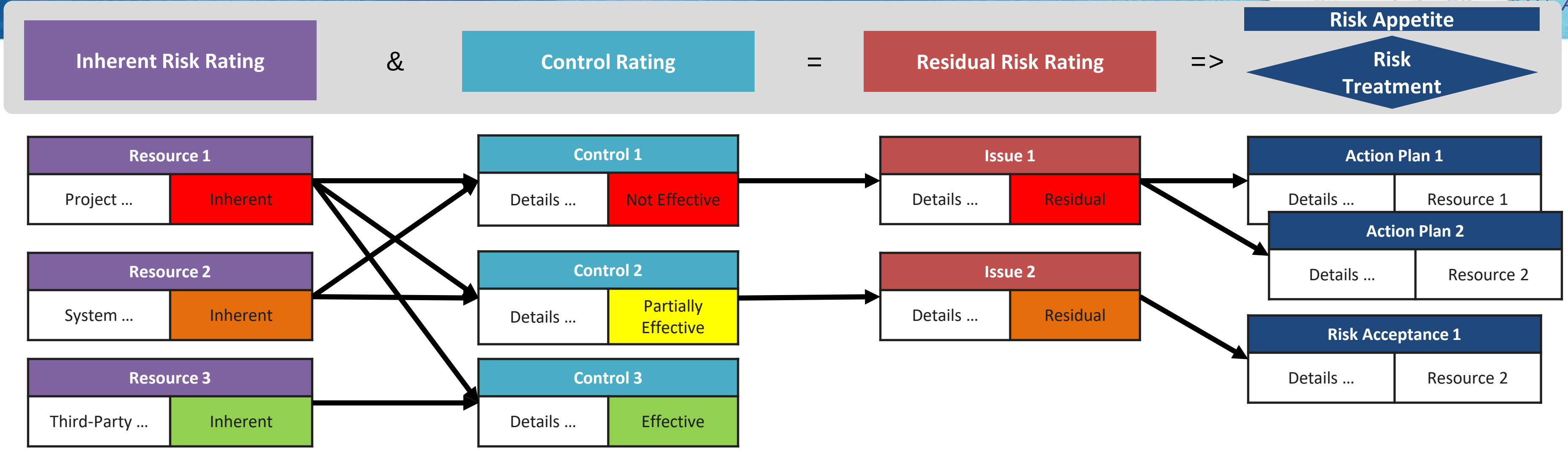
[1] Assumes revenue isn't collected during downtime and won't be recuperated afterwards

[2] Represents a relative risk for inherent risk and prioritization purposes

# Threat Event Frequency

| Frequency | | Physical and Environmental | Geopolitical |
|---|---|---|---|
| **Rare** | <0.1 | Data Center | - Australia<br>- Canada<br>- New Zealand<br>- UK<br>- US |
| **Infrequent** | ≥0.1 <1 | Server Room in Office | Select Countries in:<br>- Western Europe (e.g., Germany, Netherlands, Norway and Ireland)<br>- Latin America (e.g., Brazil, Argentina, Chile, Peru and Mexico)<br>- Asia (e.g., India and Singapore) |
| **Regular** | ≥1 <12 | Vendor Shared | Select Countries in:<br>- Eastern Europe (e.g., Ukraine and Romania)<br>- Asia (e.g., Indonesia) |
| **Very Frequent** | ≥12 | Retail Location | - OFAC Sanctioned Countries (e.g., North Korea)<br>- Other high risk countries (e.g., Russia, Venezuela, Colombia and China) |

# Risk Aggregation (Bottom Up)



Inherent Risk Rating & Control Rating = Residual Risk Rating => Risk Appetite / Risk Treatment

Resource 1: Project … | Inherent

Resource 2: System … | Inherent

Resource 3: Third-Party … | Inherent

Control 1: Details … | Not Effective

Control 2: Details … | Partially Effective

Control 3: Details … | Effective

Issue 1: Details … | Residual

Issue 2: Details … | Residual

Action Plan 1: Details … | Resource 1

Action Plan 2: Details … | Resource 2

Risk Acceptance 1: Details … | Resource 2

Risk Aggregation

**Hierarchy**

Resource

Environment

Process Level 2

Process Level 1

Business Unit

Legal Entity

**Control Taxonomy**

Control Objective

Control Type

Control Instance

Control Category

Control Domain

**Risk Taxonomy**

Threat Scenario

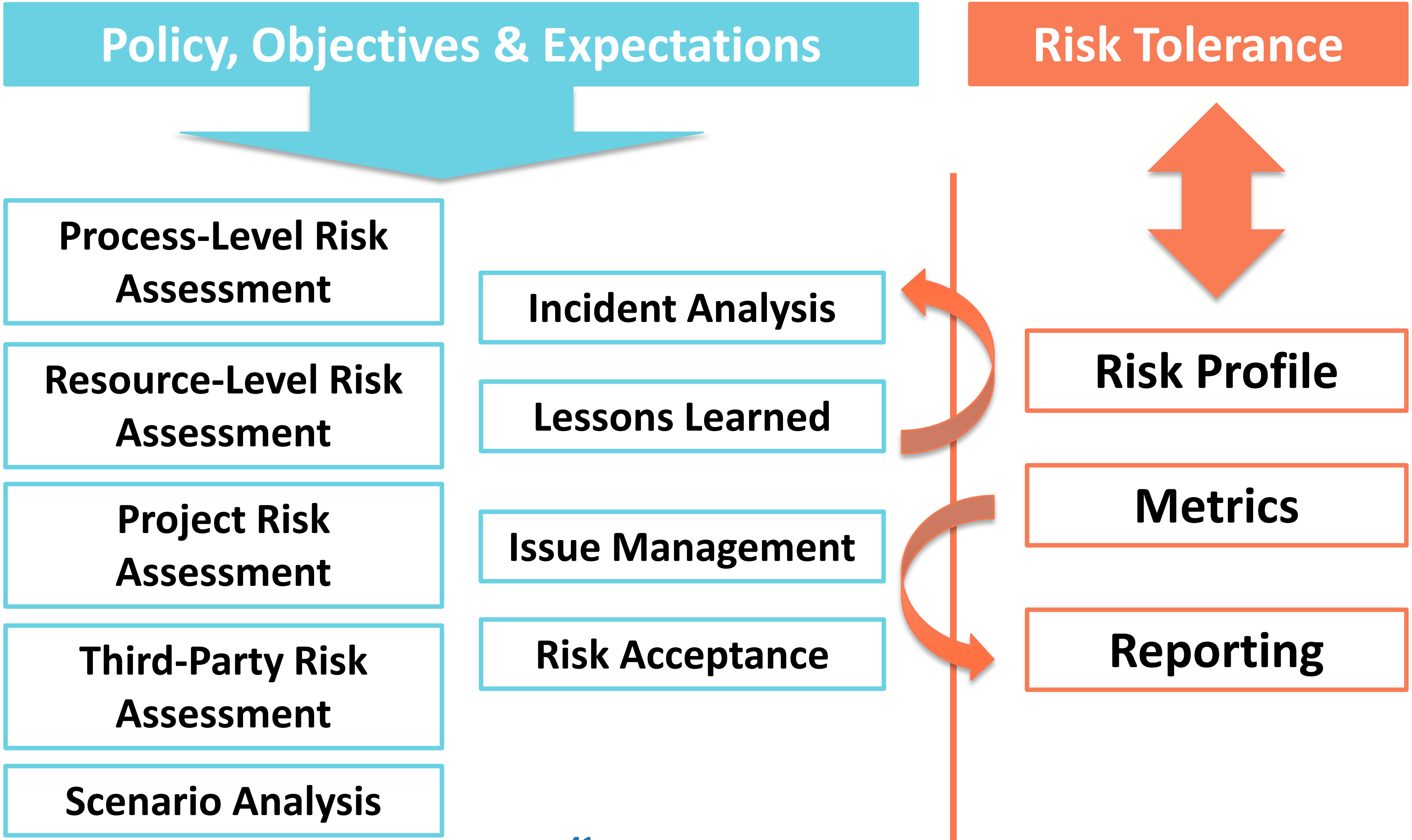
Key Risk

Risk Category

Risk Discipline

Basel Mapping

# ERM Components



Policy, Objectives & Expectations

Risk Tolerance

Process-Level Risk Assessment

Resource-Level Risk Assessment

Project Risk Assessment

Third-Party Risk Assessment

Scenario Analysis

Incident Analysis

Lessons Learned

Issue Management

Risk Acceptance

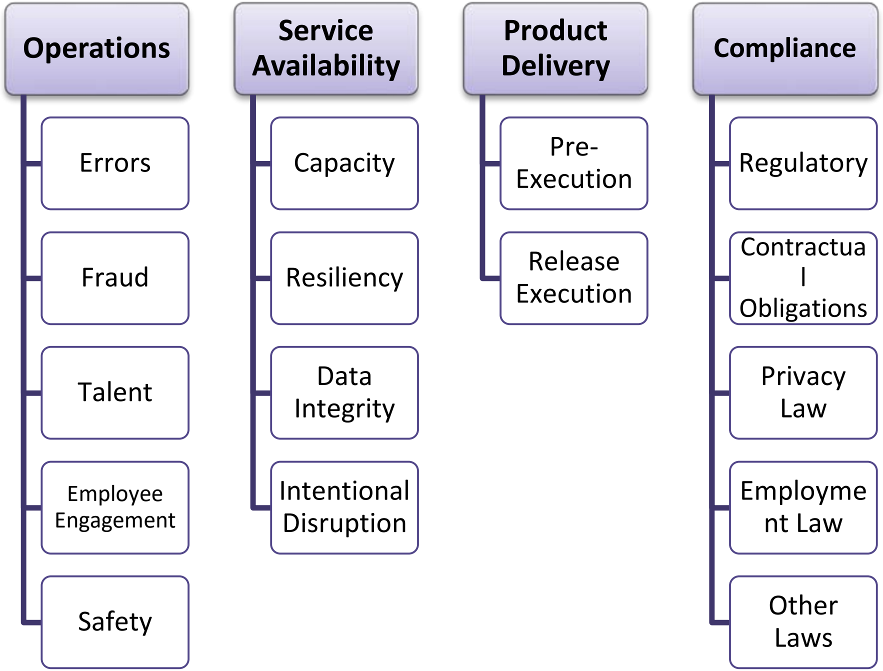
Risk Profile

Metrics

Reporting

# Applying an Enterprise-Aware Model

1. Reposition cyber threats across all operational risk domains
2. Establish a PRC library
3. Profile key business and IT processes
4. Test controls
5. Adopt loss ranges from ERM
6. Run scenario analysis workshops
7. Integrate inherent risk into IT asset inventory for prioritization



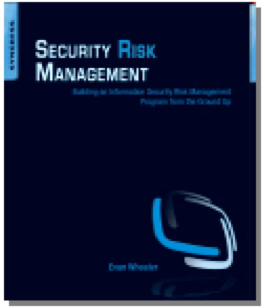
**Operations**
- Errors
- Fraud
- Talent
- Employee Engagement
- Safety

**Service Availability**
- Capacity
- Resiliency
- Data Integrity
- Intentional Disruption

**Product Delivery**
- Pre-Execution
- Release Execution

**Compliance**
- Regulatory
- Contractua l Obligations
- Privacy Law
- Employme nt Law
- Other Laws

# Recommended Reading


Security Risk Management
Building an Information Security Risk Management Program from the Ground Up
Evan Wheeler

**Security Risk Management: Building an Information Security Risk Management Program from the Ground Up**

- ISBN: 9781597496155
- Amazon Link: http://amzn.to/hyrMvC

## Questions?

**Measuring and Managing Information Risk: A FAIR Approach**

- ISBN: 978-0124202313
- Amazon Link: http://amzn.com/0124202314