# Risk Assessment and Business Impact Analysis using PMI

Michael C. Redmond
EFPR Group IT & GRC Consulting and Audit
Director, Lead Strategic Consultant and Auditor

EFPR GROUP LLP
IT & GRC Consulting and Audit

Dr. Michael C. Redmond, PhD, MBA,
MBCP, FBCI,CEM,MBA

- Ms. Redmond was the Attaché to Chile at the request of the President of Chile..
- Ms. Redmond was on the UN Council for International Disaster Recovery and spoke at a UN press conference in Belgium.
- Ms. Redmond has been an Adjunct  Professor at New York University, John Jay Graduate School, University of Maryland ( Overseas Program) and Mercy College
- LTC US ARMY 4 years Active Duty and 181/2 National Guard and Reserves
- Past experience includes Chubb, Deloitte, KPMG, Redmond Worldwide

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Dr. Michael C. Redmond, PhD

**Degrees**
- MBA PhD
-

**Certified as Lead Implementer:**
- ISO/IEC 27001 Information Security Management
- ISO/IEC 27032 Lead Cyber Security Manager
- ISO/IEC 27035 Security Incident Response
- ISO/IEC 22301 Business Continuity Management Systems
- ISO/IEC 21500 Lead Project Manager
- ISO/IEC 41001 Environmental Management
- ISO 31000 Risk Management
-

**Certified Implementer - Foundation**
- ISO 22316 Resiliency Management
- ISO 22320 Emergency Management

**Certified as Lead Auditor:**
- ISO/ IEC 27001 Information Security Management
- ISO/IEC 22310 Business Continuity Management Systems
- ISO/IEC 41001 Environmental Management

**Other Certifications:**
- Masters Business Continuity Planning (Disaster Recovery Institute) – MBCP
- Master Business Continuity Planning (Business Continuity Institute) – FBCI
- Certified Emergency Manager – CEM
- Certified Project Manager – PMP
- Certified Trainer PECB

EFPR GROUP LLP
IT & GRC Consulting and Audit

# PMI PMBOK Ten Knowledge Areas

- Project Integration Management
- Project Scope Management
- Project Time Management
- Project Cost Management
- Project Quality Management
- Project Human Resource Management
- Project Communications Management
- Project Risk Management
- Project Procurement Management
- Project Stakeholders Management

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Risk Assessment and Impact Analysis

- Risk assessments are conducted across the whole organization. They cover all the possible risks that information could be exposed to, balanced against the likelihood of those risks materializing and their potential impact – Impact Analysis.
- Once the risk assessment has been conducted, the company needs to decide how it will manage and mitigate those risks, based on allocated resources and budget

EFPR GROUP LLP
IT & GRC Consulting and Audit

# RISK According to PMBOK

- A **Risk** is an uncertain event or condition that if it occurs, has a positive or negative effect  PMBOK
- **Risk Management** is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.
- If the probability is 1, it is an issue. This means that risk is already materialized. If the probability is zero, this means that risk will not happen and should be removed from the risk register

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Known Versus Unknown Risks

- Known risks are those which can be identified and analyzed beforehand in such a way as to be able to
  - a) reduce the likelihood of their occurrence,
  - or b) plan a risk response to reduce their impact in the event that they occur

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Two Components

- Remember that risk has two components, the uncertainty of an event, which is measured by its probability, and its potential impact on the project

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Risk Process

- Determine the Organization's Vulnerability to Loss Potentials
  - Identify primary threats the organization may face, and secondary/collateral events that could materialize because of such threats Select vulnerabilities most likely to occur and with greatest impact

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Risk Process

- Identify Controls and Safeguards to Prevent or Minimize the Effect of the Loss Potential
  - Review previous actions taken and mitigations installed to reduce the probability of incidents that would
    - Physical protection
      - Understand the need to restrict access to buildings, rooms, and other enclosures where circumstances demand a "3-dimensional" consideration

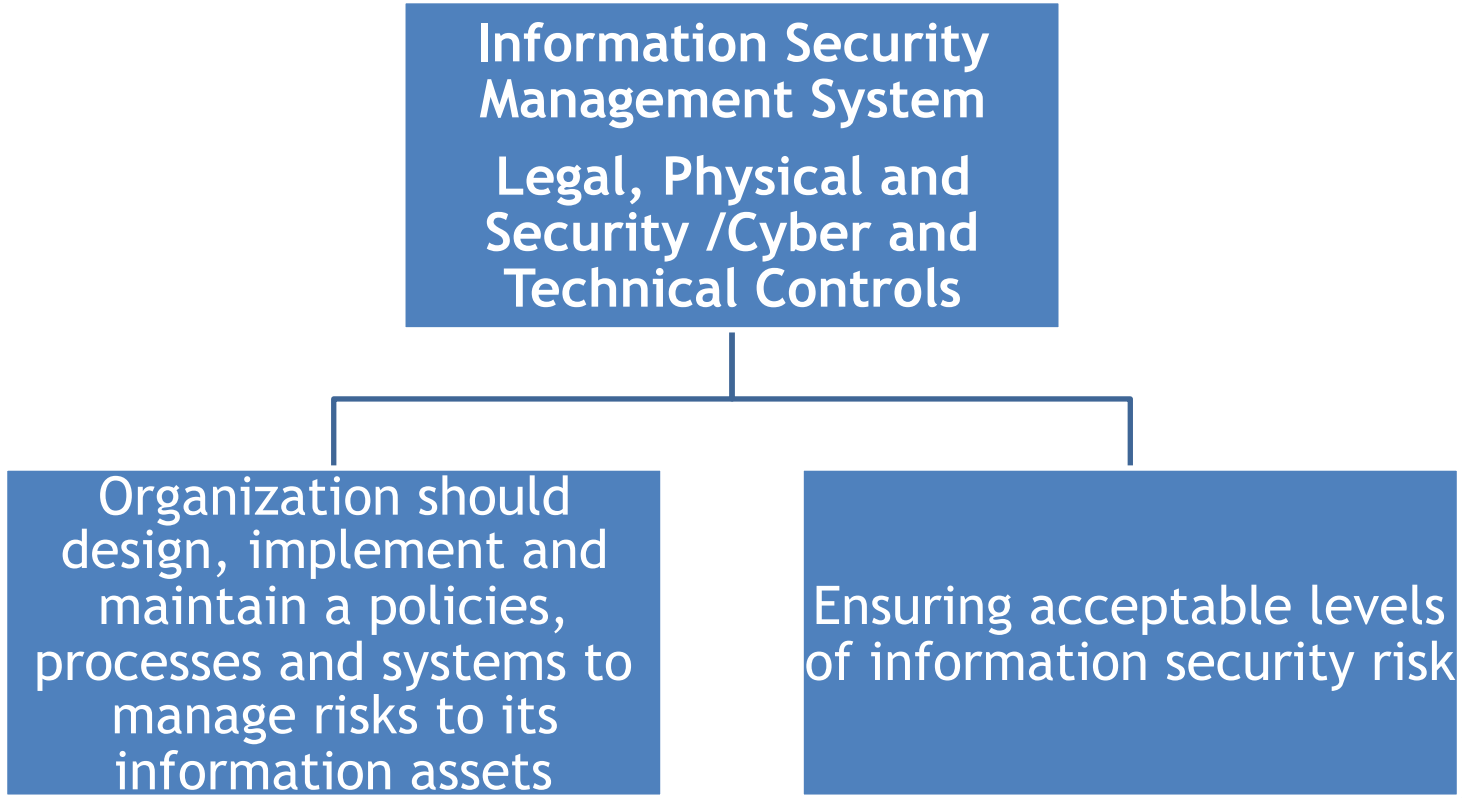
EFPR GROUP LLP
IT & GRC Consulting and Audit

# ISO 27001 Risk Assessments

- **ISO 27001 Risk Assessments.** ISO 27001 is the international Standard that sets out the specifications of an Information Security Management System (ISMS), a best-practice approach to addressing information security that encompasses people, process and technology

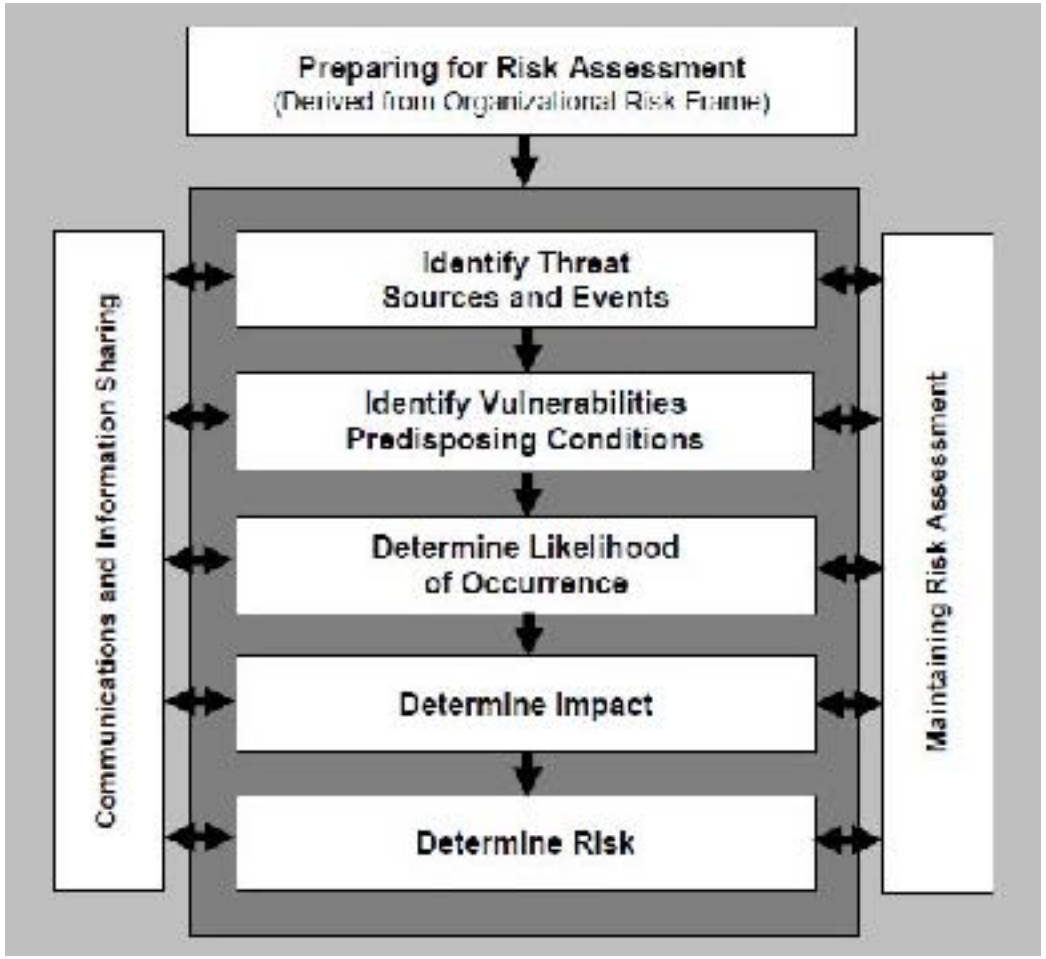
EFPR GROUP LLP
IT & GRC Consulting and Audit

# Risk Assessment using ISO 27001 ISMS framework




EFPR GROUP LLP
IT & GRC Consulting and Audit

# Risk Process Steps




EFPR GROUP LLP
IT & GRC Consulting and Audit

# Define your risk assessment methodology

- These are the rules governing how you intend to identify risks, to whom you will assign risk ownership, how the risk's impact on the confidentiality, availability and integrity of the information will be measured, and the method of calculating the estimated impact and likelihood of the risk occurring.

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Compile a list of information assets

- An asset-based risk assessment presents a more robust risk assessment process. It will be easiest to work from an existing list of information assets, which includes hard copies of information, electronic files, removable media, mobile devices, and intangibles such as intellectual property.

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Identify threats and vulnerabilities

- Identify the threats and vulnerabilities that apply to each asset.
- For instance, the threat could be ‘theft of mobile device’, and the vulnerability could be ‘lack of formal policy for mobile devices’.

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Qualify the extent of the risk

- Assign impact and likelihood values of the risk coming to pass (based on your risk criteria)

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Mitigate the risks to reduce them to an agreed, acceptable level

- ‘Terminate’ (or avoid) the risk by eliminating it entirely.
- ‘Treat’ the risk by applying security controls.
- ‘Transfer’ the risk to a third party.
- ‘Tolerate’ the risk.

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Controls

- Information security policies.
- Organization of information security.
- Human resources security.
- Asset management.
- Access control.
- Cryptography.
- Physical and environmental security.
- Operational security.
- Communications security.
- System acquisition, development and maintenance.
- Supplier relationships.
- Information security incident management.
- Information security aspects of business continuity management.
- Compliance.

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Compile risk reports

- **Statement of Applicability (SoA)**
  The SoA should set out a list of all controls recommended by Standard or Regulation, together with a statement of whether or not the control has been applied, and a justification for its inclusion or exclusion.
- **Risk treatment plan (RTP)**
  The RTP describes how the organization plans to deal with the risks identified in the risk assessment.

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Review, monitor and audit

- Continually review, update and improve the ISMS to make sure it is functioning optimally, and adjusts to the constantly changing threat environment.
- One aspect of reviewing and testing is an internal audit. This requires the ISMS manager to produce a set of reports that provide evidence that risks are being adequately treated.

EFPR GROUP LLP
IT & GRC Consulting and Audit

# PDCA


EFPR GROUP LLP
IT & GRC Consulting and Audit

# Risk Checklist

Evaluate impact of risks and threats on those factors essential for conducting business operations: availability of personnel, availability of information technology, availability of technology, status of infrastructure

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Risk Checklist

Evaluate risks and classify them according to relevant criteria, including: risks under the organization's control, risks beyond the organization's control, threats with prior warnings, and threats with no prior warnings.

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Risk Checklist

Evaluate controls and recommend changes, if necessary, to reduce impact due to risks and threats

Controls to inhibit impact threats: preventive controls

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Business Impact Analysis

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Assess Effects of Disruptions and Business Impact

1. Quantitative
2. Qualitative

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Determine Loss Exposure

Quantitative

- Data Loss
- Revenue loss
- Fines
- Legal liability
- Additional expenses/increased cost of working

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Determine Loss Exposure

Qualitative

- Human resources
- Morale
- Confidence
- Legal
- Social and corporate image
- Financial community credibility

EFPR GROUP LLP
IT & GRC Consulting and Audit

# How does a firm without any plans start?

- ‘Plan-Do-Check-Act’ model
  - Risk Assessments
  - Business Impact Analysis (BIA)
  - Strategic Planning
  - Documenting Plans
  - Testing and Exercises
  - Training
  - Maintenance

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Accomplish Goals With Schedule Outlined in Proposal

9 .

## 5.0 Project Schedule

**Phase 1 Deliverables:**

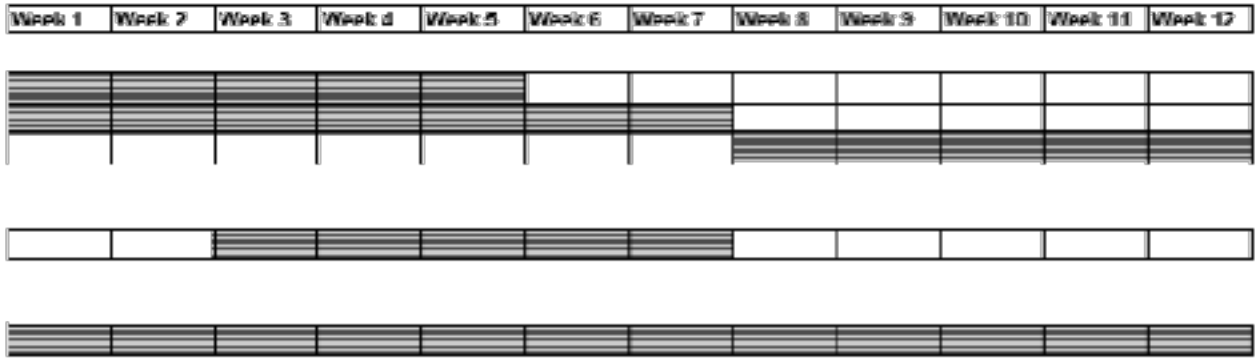
1.1 Business Impact Assessment
1.2 Risk Analysis
1.3 Business Continuity Strategy Document for Executive Management

**Phase 2 Deliverables:**

2.1 Develop governance policies, processes and procedures.

**Phase 3 Deliverables:**

3.1 Develop templates and processes for Business Continuity Planning, train and mentor staff in their use and develop flexible Business Continuity drill procedures.




EFPR GROUP LLP
IT & GRC Consulting and Audit

# Define Risk and Impact Scope
# Information Security …

# Risk Analysis (RA)

- Components
  - Identify, analyze and document Potential Risks to the Organization
  - Identify, analyze and document Outside Expertise Required
  - Identify, analyze and document Vulnerabilities/Threats/Exposures
  - Identify, analyze and document Risk Reduction/Mitigation Alternatives
  - Identify, analyze and document Credible Information Sources
  - Analyze and Document Loss Potentials
  - Identify, analyze and document the probability of events
  - Identify, analyze and document the Organization's Vulnerability to Loss Potentials

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Risk Process

- Analyze and Document the Function of Probabilities and Risk Reduction/ Mitigation Within the Organization
- Identify, analyze and document Potential Risks to the Organization
- Probability
- Consequences
- Identify, analyze and document Outside Expertise Required
- Identify, analyze and document Vulnerabilities/Threats/Exposures
- Identify, analyze and document Risk Reduction/Mitigation Alternatives
- Identify, analyze and document Credible Information Sources
- Interface with Management to Identify, analyze and document Acceptable Risk Levels
- Document and Present Findings

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Risk Analysis (RA)

- Rigor and Techniques of RA
- Benefits of RA
- Components of RA
- Likely and unlikely risk
- Effects of existing controls in mitigating the risk
- What recommendations might be made to further the risk

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Business Impact Analysis (BIA)

- Components
  - Identify, analyze and document alternative risk analysis methodologies and tools
  - Identify, analyze and document and Implement Information Gathering Activities
  - Identify, analyze and document Organization Functions
  - Identify, analyze and document and Define Criticality Criteria
  - Identify, analyze and document Interdependencies
  - Identify, analyze and document Information Requirements
  - Identify, analyze and document Resource Requirements
  - Identify, analyze and document Training requirements
  - Identify, analyze and document Loss Exposure
  - Identify, analyze and document data analysis methods (manual or computer)

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Business Impact Analysis (BIA)

- Components (Continued)
  - Identify, analyze and document critical functions
  - Business functions
  - Identify, analyze and document vital records to support business continuity and business restoration
  - Identify, analyze and document Recovery Timeframes and Minimum Resource Requirements
  - Identify, analyze and document Business Processes
  - Identify, analyze and document Replacement Times
  - Identify, analyze and document Viable Recovery Strategies with Business Functional Areas
  - Identify, analyze and document Business Continuity Strategy Requirements
  - Identify, analyze and document alternative recovery strategies
  - Effectively analyze business needs criteria
  - Clearly define recovery planning objectives

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Business Continuity Strategy

- How BIA and RA inform the Strategy
- Components of Strategy (next slide)
- How Executive Management can demonstrate benefits realized from Exec Strategy
- Organizational Change Management component
- How work effort Initial and Maintenance will be incorporated into each bus units regular workflow

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Business Continuity Strategy

- Components of Thinking
  - Identify, analyze and document the Existence of Appropriate Emergency Response Procedures
  - Identify, analyze and document Components of Emergency Response Procedure
  - Analyze and Document implications of statutory regulations
  - Identify, analyze and document examples of alternative plans and structures
  - Identify, analyze and document tasks to be undertaken
  - Define Business Continuity Procedures
  - Identify, analyze and document which information should be duplicated
  - Identify, analyze and document suitable storage facilities
  - Analyze and Document retention periods
  - Identify, analyze and document key suppliers
  - Information recovery
  - Cost Benefit Analysis

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Business Continuity Strategy

- Components of Process
  - Identify, analyze and document Business Continuity Strategy Requirements
  - Review business recovery issues
  - Review technology recovery issues for each support service
  - Review non-technology recovery issues for each support service, including those support services not dependent upon technology
  - Compare internal/external solutions
  - Identify, analyze and document alternative recovery strategies
  - Compare internal and external solutions Assess risk associated with each optional recovery strategy
  - Assess Suitability of Alternative Strategies Against the Results of a Business Impact Analysis

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Business Continuity Strategy

- Components of Process (Continued)
  - Effectively analyze business needs criteria
  - Clearly define recovery planning objectives
  - Develop a consistent method for evaluation
  - Set baseline criteria for options
  - Prepare Cost/Benefit Analysis of Recovery Strategies and Present Findings to Senior Management
  - Employ a practical, Analyze and Documentable methodology
  - Set realistic time schedules for evaluation and report writing
  - Deliver concise specific recommendations to senior management
  - Select Alternate Site(s) and Off-Site Storage

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Governance Policies and Procedures

- Plan Maintenance
- What Levels of Management Will be Involved in Review
- What components should be maintained
- Typical Frequency for Maintenance
  - BIA, RA, Strategy and Plan
- Need for Business Units to Exercise Plan
- Which Business Units Typically Provide a Compliance Audit

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Considerations

Protect Personal Health formation (PHI), Payment Card formation (PCI) and Personally Identifiable Information (PII)

How are you penetrable?

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Cyber Attack

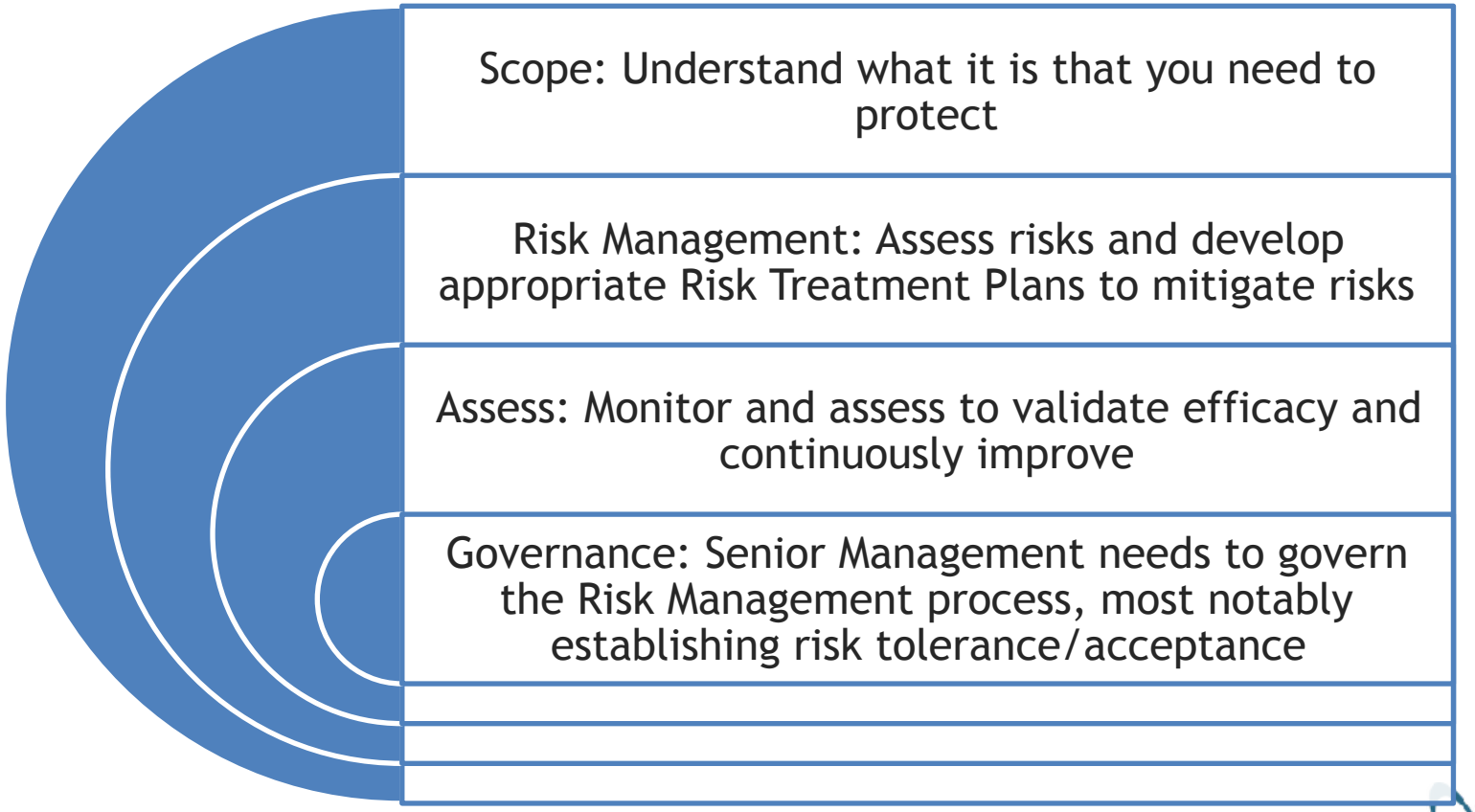
- More and more attacks are happening every day, resulting in loss of reputation, fines, legal liabilities and so much more.
- It is not IF you will be the potential victim of a Cyber Attack but When?

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Security Risk Factors

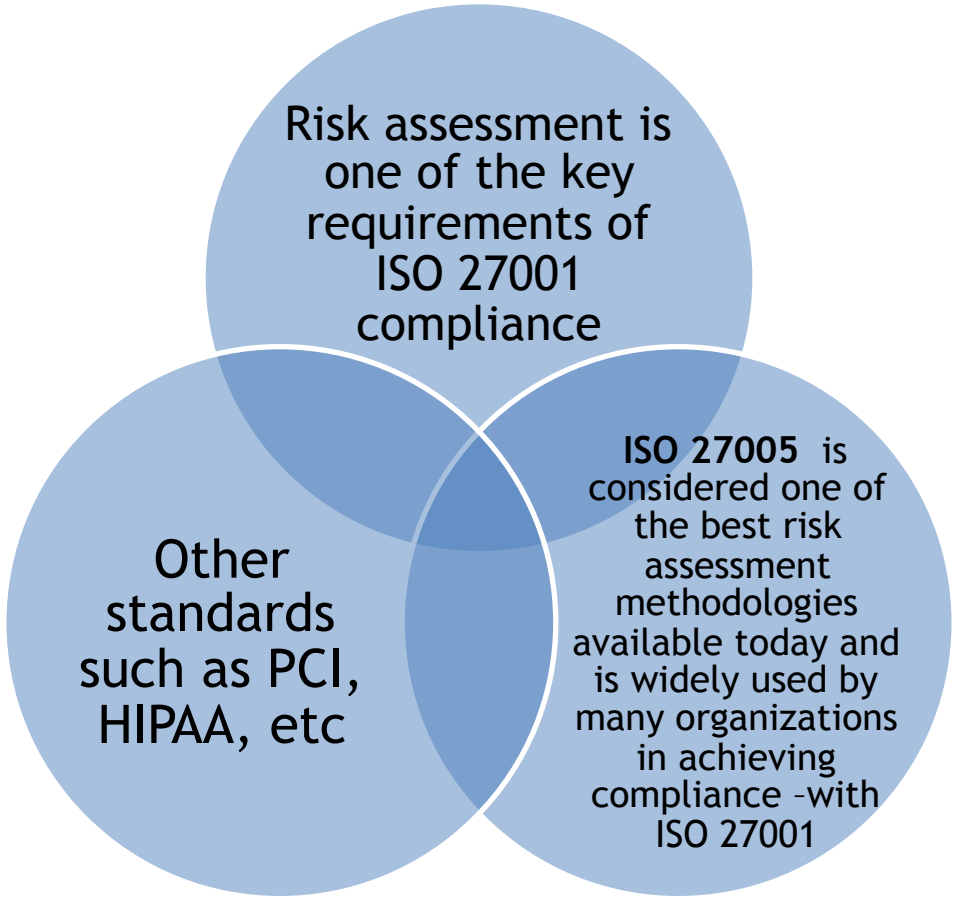

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Risk Framework




EFPR GROUP LLP
IT & GRC Consulting and Audit

# They Work Together




EFPR GROUP LLP
IT & GRC Consulting and Audit

# Risk Analysis (RA)

- Components
  - Identify, analyze and document Potential Risks to the Organization
  - Identify, analyze and document Outside Expertise Required
  - Identify, analyze and document Vulnerabilities/Threats/Exposures
  - Identify, analyze and document Risk Reduction/Mitigation Alternatives
  - Identify, analyze and document Credible Information Sources
  - Analyze and Document Loss Potentials
  - Identify, analyze and document the probability of events
  - Identify, analyze and document the Organization's Vulnerability to Loss Potentials

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Risk Analysis (RA)

- Rigor and Techniques of RA
- Benefits of RA
- Likely and unlikely risk
- Effects of existing controls in mitigating the risk
- What recommendations might be made to mitigate the risk

EFPR GROUP LLP
IT & GRC Consulting and Audit

# REWI


he Resilience based Early Warning Indicators (REWI) method is a collection of self-assessment measures

rovides information about an organization's resilience.


The primary goal of the method is to generate early warnings that improve the rganization's ability and performance in the long run.

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Resilience Attribute: Risk Awareness

- The *risk awareness* attribute measures the degree of risk understanding, as well as anticipation regarding what to expect and attention so as to know what to look for. In a security incident management context these contributing success factors can be expanded into general issues

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Risk understanding

- To what degree we understand the security risks associated with the system. Risk understanding can be understood by asking questions (the “general issues”)

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Understanding

- *Do we have knowledge about the* information and communication technologies (ICT) *system and its components?*
- A (correct) understanding of how the system work will provide insight into how it may be attacked and the possible consequences.


EFPR GROUP LLP
IT & GRC Consulting and Audit

# Risks Understanding

- *Do we have personnel with information security competence?* Whether the employees are security aware or not will affect the security risks.
- *Do we report on security incidents?* Information about past incidents will provide insight into what may go wrong in the future.
- *Do we have appropriate defense mechanisms?* Information about the technical safeguards gives knowledge about

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Protection

How well the system is protected.

- *Is the organization's security policy efficient?*
- Insight in to what degree the security policy is implemented into the organization and whether it is followed by the employees will influence the efficiency of the technical safeguards and barriers.

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Anticipation

What security incidents we can expect

- *Do we have updated knowledge about relevant threats?* A systematic and regular identification of vulnerabilities and threats is necessary in order to understand what may go wrong.
- *Do we learn from experience?* The organization's past experiences is a valuable source of information.

You want to avoid reoccurrence of security incidents and to learn from its own success stories ("what went right").

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Response

Response: To what degree the organization is prepared to respond to security incidents.

- *Do we have personnel with the ability to handle incidents?* There must be employees who are capable of handling
- the incidents, including making critical decisions.
- *How do we train on dealing with potential incidents?* Training on potential scenarios is essential in order to
- know what to do, both with respect to expected and unexpected events. The training scenarios should be regularly
- reviewed and adapted, in order to reflect the current threat picture as accurately as possible.

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Robustness

Robustness of response: To what degree the organization can respond to security incidents, without suffering damage.

- *Do we have sufficient redundancy in skills among the employees?*
- Organizations that ensure that the employees are redundant in skills, or possess multiple skills, are more likely to successfully handle incidents that go beyond the planned or foreseen.
- *Do we have sufficient backup capacity / redundancy for the necessary critical functions?* Fault tolerance, redundancy and recovery are important aspects for preserving the organization's critical functions
- *Is the communication between involved actors sufficient?* During incident response it is crucial that all involved
- are able to communicate, without misunderstandings or confusions
- *Do we manage incidents in compliance with existing policies?* A robust response require compliance with existing
- policies and best practices.

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Resourcefulness

Resourcefulness : To what degree the organization can ensure timely and sufficient response.

- *Does the incident response team have sufficient resources?* There must be a sufficient number of personnel assigned to the different roles in the incident response team, including back-up personnel in case of unavailability, and the response team must be capable of solving their tasks in a timely manner.
- *Do we have adequate IT systems to support timely updating of necessary information?* A timely response requires timely updating necessary information and communicating this to all involved actors.

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Resilience Attribute: Support

- The *support* attribute measures the presence of an established support systems, so that when faced with tough decisions or tradeoffs there is some kind of decision support or help that is institutionalized and part of practice .
- In addition, support includes the ability to uphold critical support functions (technical, human and organizational resources) in case of disruption is essential (redundancy)

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Management Context

In a security incident management context these contributing success factors can be expanded into the following general issues:

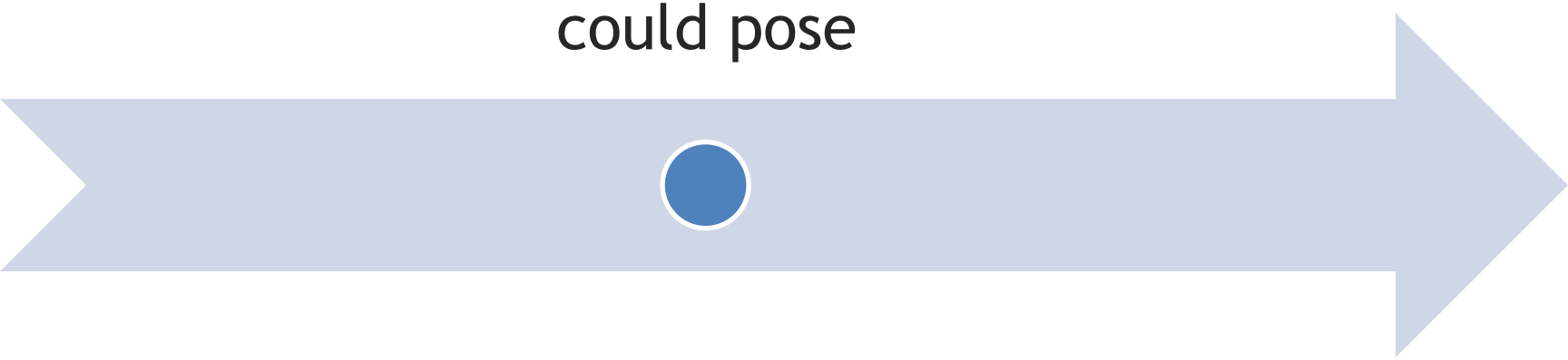
- Decision support: To what degree the organization support the trade-off between security and production.
- *Do we have adequate decision support staffing?* Efficient incident response will require available personnel with knowledge, experience and authority to make decisions.
- *Do we have adequate ICT decision support systems?* Efficient incident response will often require adequate support systems in place, including support for the support systems themselves.
- *Do we have adequate external support?* Security incident management often requires support om external actors,such as anti-virus and third party software providers.

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Technical Questions

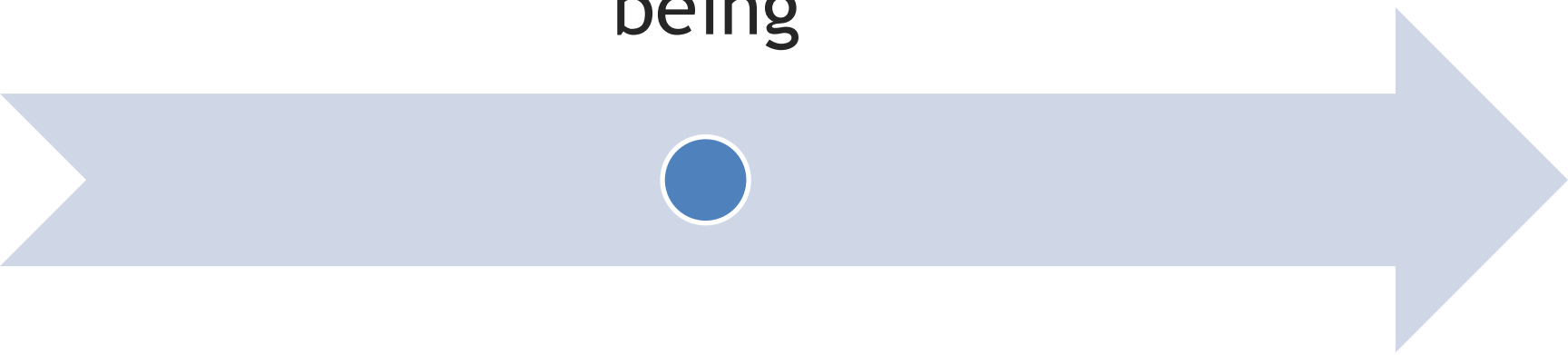
- **Authentication Servers:** Authentication servers, including directory servers and single sign-on servers, typically log each authentication attempt, including its origin, username, success or failure
- **Remote Access Software:** Remote access is often granted and secured through virtual private networking (VPN). VPN systems typically log successful and failed login attempts, as well as the dates and times each user connected and disconnected, and the amount of data sent and received in each user session. VPN systems that support granular access control, such as many Secure Sockets Layer (SSL) VPNs, may log detailed information about the use of resources.
- **Vulnerability Management Software:** Vulnerability management software, which includes patch management software and vulnerability assessment software, typically logs the patch installation history and vulnerability status of each host, which includes known vulnerabilities and missing software updates.5 Vulnerability management software may also record additional information about hosts' configurations. Vulnerability management software typically runs occasionally, not continuously, and is likely to generate large batches of log entries.
- **Web Proxies:** Web proxies are intermediate hosts through which Web sites are accessed. Web proxies make Web page requests on behalf of users, and they cache copies of retrieved Web pages to make additional accesses to those pages more efficient. Web proxies can also be used to restrict Web access and to add a layer of protection between Web clients and Web servers. Web proxies often keep a record of all URLs accessed through them.

Identify the assets, consider the threats that could compromise those assets, and estimate the damage that the realization of any threat could pose



EFPR GROUP LLP
IT & GRC Consulting and Audit

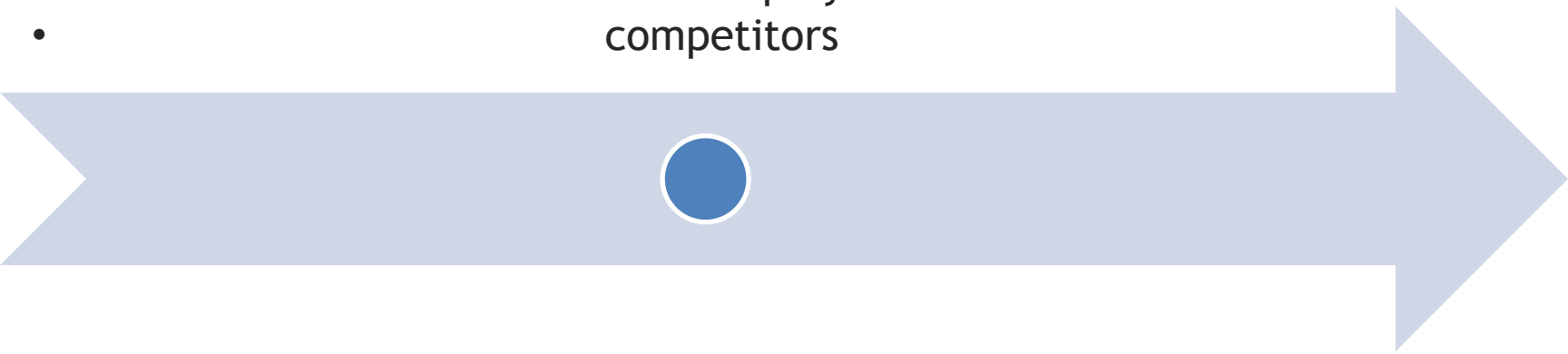
# What risk would Losing trade secrets pose to your company's financial well being



EFPR GROUP LLP
IT & GRC Consulting and Audit

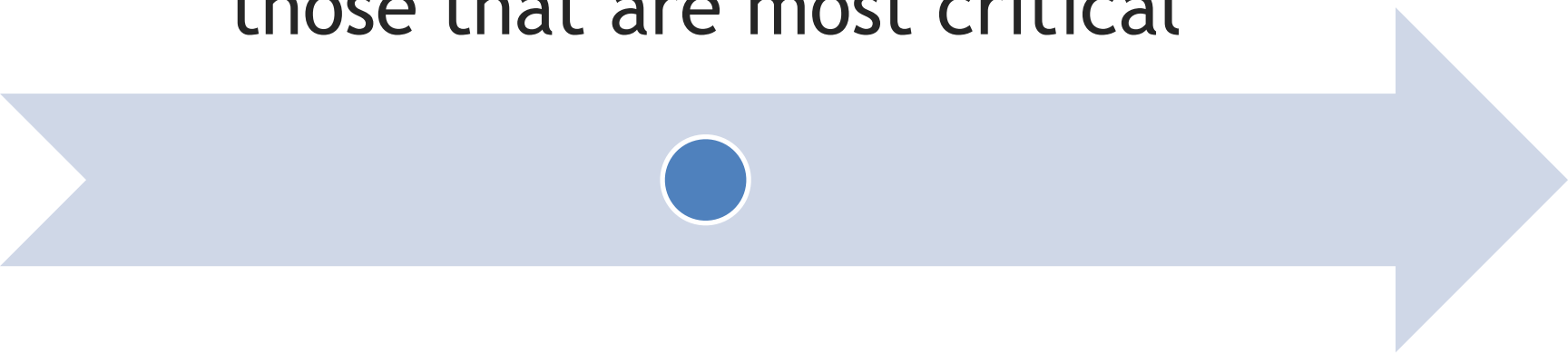
# Identify the various entities that pose threats to your company's well being –

- hackers
- disgruntled employees
- careless employees
- competitors



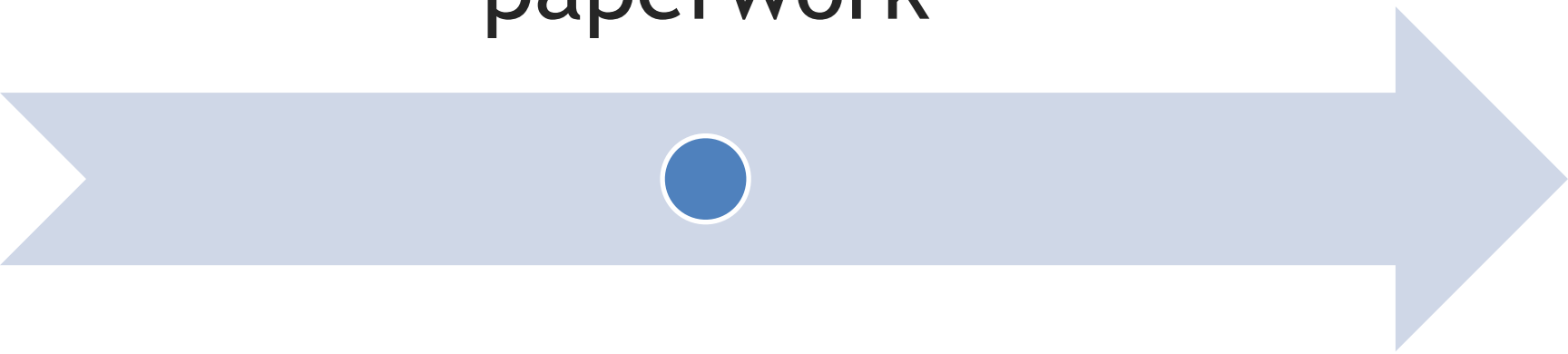
EFPR GROUP LLP
IT & GRC Consulting and Audit

Identify the assets that you are trying to protect with special attention to those that are most critical



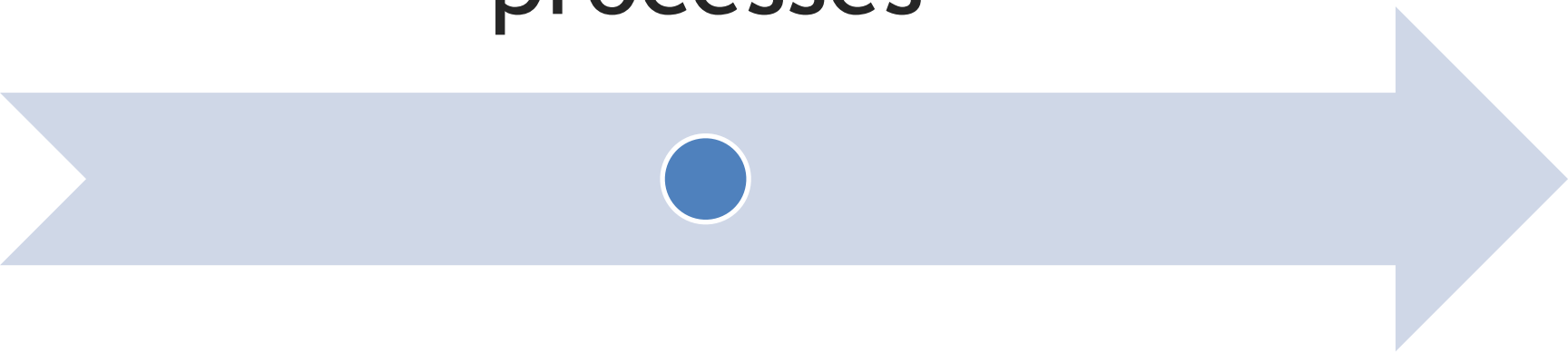
EFPR GROUP LLP
IT & GRC Consulting and Audit

# Consider all assets from automated systems to paperwork



EFPR GROUP LLP
IT & GRC Consulting and Audit

# What are the weakest links in your systems and processes



EFPR GROUP LLP
IT & GRC Consulting and Audit

# Make a list of possible vulnerable targets

- Source Code
- Engineering Drawings
- Patent Applications
- Customer Lists
- Contracts
- Admin Passwords
- Data Centers
- UPS Devices
- Firewalls
- Payroll Records

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Next Step

Assign numeric values to those risks

Calculated risk values provide a basis for determining how much time and money to invest in protecting

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Risk and Impact

Likelihood (probability) is a measure of how likely a loss is to happen

Impact (severity) is how much damage will be done to the organization if the loss occurs

EFPR GROUP LLP
IT & GRC Consulting and Audit

# FMEA

Failure mode effects analysis (FMEA) measure of the effectiveness of current controls

Formula is:

- :ikelihood that a threat is acted on (independent of your precautions against it) times the anticipated damage (impact) times the effectiveness of your efforts in mitigating the risks (controls).

EFPR GROUP LLP
IT & GRC Consulting and Audit

# Thanks

Ms. Michael C. Redmond
Director
EFPR Group - IT GRC
585-340-5187
Consulting and Audit

EFPR GROUP LLP
IT & GRC Consulting and Audit