# COSO ERM

## מתיאוריה לפרקטיקה

Entropy Consultants

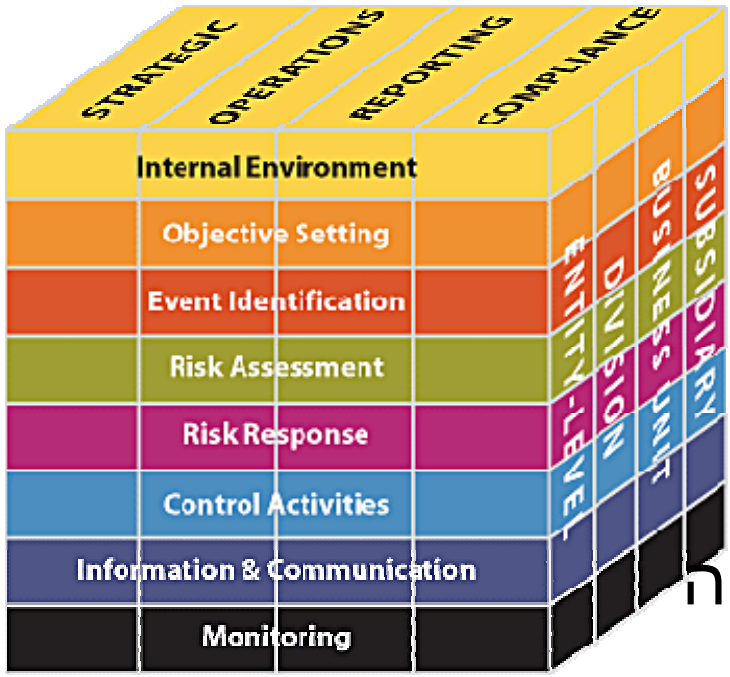
Advanced Governance Control Solutions

# הגדרת ERM על פי COSO

*"... a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."*

# COSO FRAMEWORK

- רמות העל של ה Framework הינם:
  - אסטרטגיית הארגון
  - תפעול – תהליכים, מערכות, אנשים
  - דיווח – פנימי וחיצוני
  - תאימות לחוקים ורגולציות
- פעילות ניהול הסיכונים נדרשת בכל הרבדים הארגוניים השונים
- בכל רובד יש להתייחס ל – 8 רכיבי ה Framework



# מבט על

# COSO FRAMEWORK

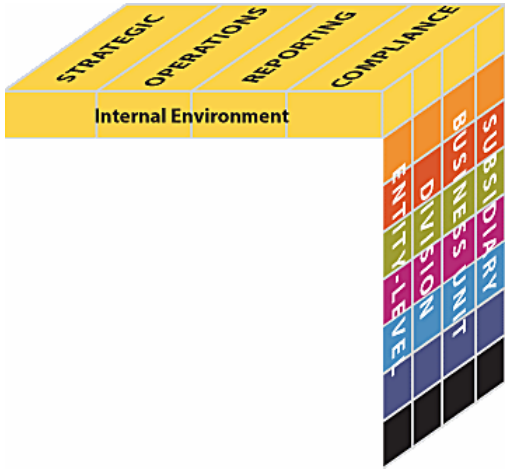
יישום של 8 המרכיבים מבטיח קיום
מערך ניהול סיכונים אפקטיבי

# כלים למימוש

## COSO ERM Framework

# סביבה ארגונית (סביבת הבקרות) - תיאוריה

- הגדרה של מדיניות ניהול סיכונים כלל ארגונית
- פיתוח של תרבות ניהול סיכונים – Risk Culture
- יש לשקול כיצד התנהגות הארגון היום יומית משפיעה על ה – Risk Culture



# סביבה ארגונית - פרקטיקה

- הגדר והפץ הצהרת הנהלה בנושא ניהול סיכונים תפעוליים (נגזרת ממדיניות ניהול הסיכונים)
- הגדר מדדים לבחינת ה Risk Culture של הארגון
- הגדר שלבי התקדמות בהטמעה ואופן מדידתם
- חבר מערכות טכנולוגיות לתמיכה בתהליכי ההטמעה של מדיניות ניהול הסיכונים
- קיים סקרים פנים ארגוניים לבחינת רמת ה Risk Culture והעלאת המודעות (Awareness)

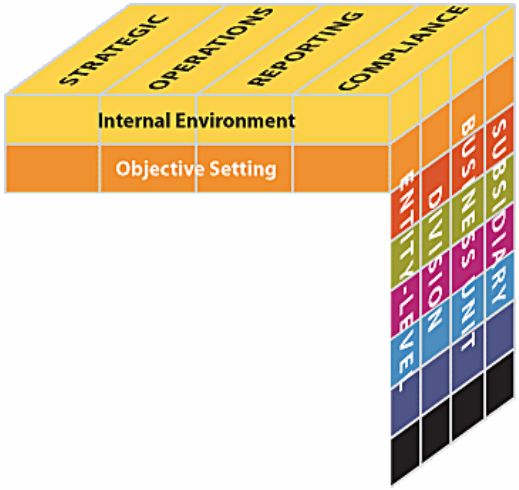
**Exhibit 2.5**
**Illustrative Risk-Related Culture Survey**

| # | Question | Attribute | Mean Rating | | Std Dev | Count | SD | D | N | A | SA |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | The leaders of my unit set a positive example for ethical conduct | Leadership and Strategy | 1.42 | Strong | 0.71 | 186 | 1 | 3 | 9 | 77 | 96 |
| 2 | I understand the entity's overall mission and strategy | Leadership and Strategy | 1.05 | Good | 0.69 | 186 | 0 | 7 | 18 | 119 | 42 |
| 3 | Disciplinary action is taken against those who engage in professional misconduct | Accountability and Reinforcement | 0.21 | Action Needed | 1.20 | 175 | 11 | 55 | 18 | 68 | 23 |
| 4 | Turnover of personnel has not significantly affected our ability to achieve objectives | People and Communication | 0.81 | Caution | 0.88 | 145 | 4 | 3 | 39 | 69 | 30 |
| 5 | The leaders of my business unit are receptive to all communications about risk, including bad news | Risk Management and Infrastructure | 0.99 | Good | 0.85 | 183 | 2 | 13 | 16 | 106 | 46 |

In the example above, each question is ranked using a scale of -2 to +2 as follows: -2 Strongly Disagree (SD); -1 Disagree (D); 0 Neutral (N); +1 Agree (A); +2 Strongly Agree (SA). The assessment, depicted by the color coding, is based on the mean ratings. Additional information is provided by the standard deviation, which is a measure of the respondents' degree of consensus around an issue – the smaller the standard deviation, the greater the respondents' level of agreement on that issue, and the greater the standard deviation, the less agreement.

# הגדרת מטרות - תיאוריה

- שילוב פרקטיקת ניהול סיכונים תפעוליים במטרות המרכזיות של הארגון
- הגדרת רמת ה RISK הכוללת של כל הארגון - Risk Appetite המקובלת על
  - דירקטוריון הארגון
  - הנהלת הארגון
- הגדרת רמת ה – Risk Tolerance עבור מדדי הארגון הרלוונטים

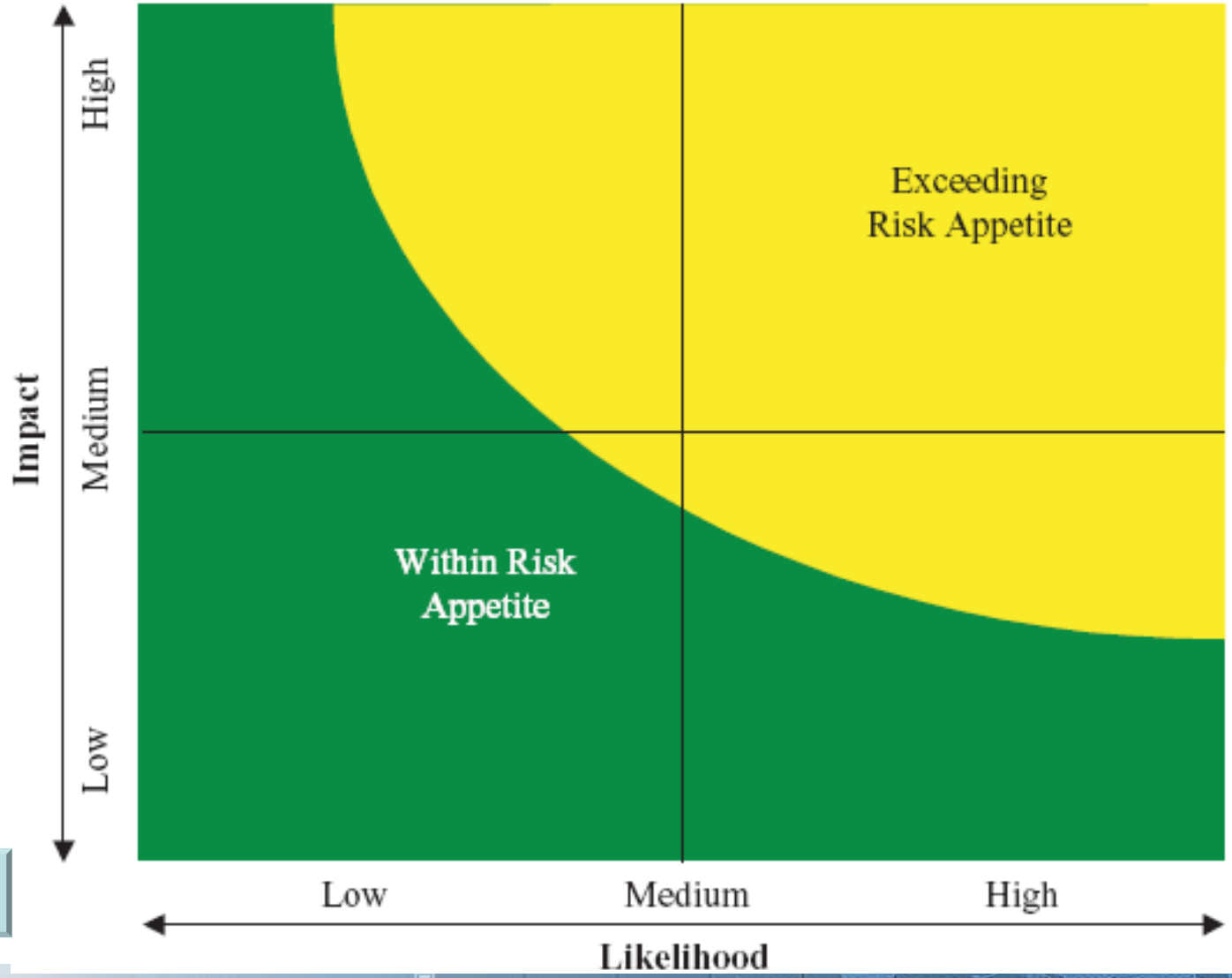


# הגדרת מטרות - פרקטיקה

- בצע הערכת סיכונים בעת קביעת דרכי פעולה למימוש המטרות המרכזיות של הארגון
- הגדר את ה Risk Appetite של הארגון באופן:
  - **איכותי** – מענה על שאלות מפתח כגון אילו נזקים אני מוכן לספוג, מאיזה מקור, באיזה היקף

  **או**
  - **כמותי** – הגדרה מתמטית של גרף ה risk appetite עבור כלל הארגון (לחץ כאן לגרף לדוגמא)
- הגדר את ה Risk Tolerance כחלק בלתי נפרד ממשימות הארגון, מטרותיו, ה - Risk Appetite של זה.

# הגדרה כמותית – Risk Appetite



## Mission

**To be a leading producer of premium household products in the regions in which we operate**

### Strategic Objectives

- To be in the top quartile of product sales for retailers of our products

**Measures**

1. Market share

### Strategy

Expand production of our top-five selling retail products to meet increased demand

### Related Objectives

- Increase production of Unit X by 15% in the next 12 months
- Hire 180 qualified new staff across all manufacturing divisions
- Maintain product quality of 4.0 sigma
- Maintain 22% staff cost per dollar order

**Measures**

- Units of production
- Number of staff hired
- Product quality by sigma

### Risk Appetite

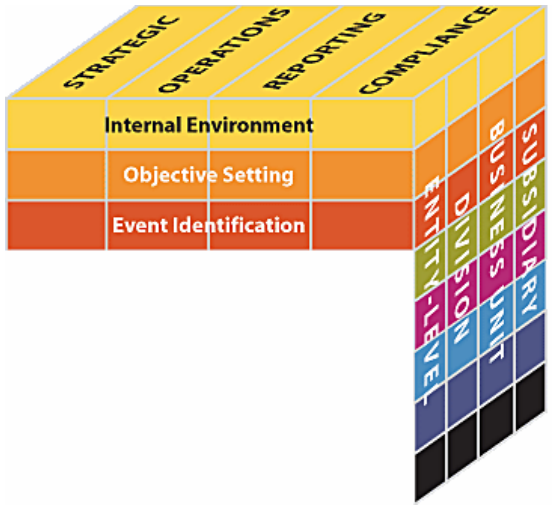
- Accept that the company will consume large amounts of capital investing in new assets, people and process
- Accept that competition could increase (e.g., through predatory pricing, etc.) as we seek to increase market share, thereby reducing profit margins
- We do not accept erosion of product quality

### Risk Tolerances

| Measure | Target | Tolerances – Acceptable Range |
|---|---|---|
| Market share | 25th percentile | 20% – 30% |
| Units of production | 150,000 units | -7,500/+10,000 |
| Number of staff hired (net) | 180 staff | -15/+ 20 |
| Product quality index | 4.0 sigma | 4.0 – 4.5 sigma |

# זיהוי אירועים - תיאוריה

- למד להבדיל בין סיכונים להזדמנויות
- אירועים בעלי השפעה שלילית מהווים סיכון
- זהה אירועים חיצוניים ופנימיים היכולים להשפיע על השגת יעדי הנהלת הארגון
- הגדר כיצד גורמים חיצוניים ופנימיים משפיעים על פרופיל הסיכון ( Risk Profile) של הארגון



# זיהוי אירועים - פרקטיקה

- הגדר וקשר אירועים היכולים להשפיע על ה Risk Tolerance שהוגדר ע"י שימוש בשיטות כגון:
  - Event Inventory – בניית מאגר אירועים גנרי רלוונטי לתחום \ תהליך
  - סדנאות
  - ראיונות
  - שאלונים וסקרים
  - ניתוח התהליך או התהליכים המרכיבים תחום פעולה של הארגון
  - הגדרת Leading Risk Indicators ו Escalation Triggers (לדוגמא: ▶ )
  - ניהול מאגר אירועים (Loss Data Events) חיצוני ו \ או פנימי (לדוגמא: ▶ )
- אחד אירועים לטובת טיפול וזיהוי יעיל של הזדמנויות \ סיכונים. (לדוגמא: ▶ )

# Leading Risk Indicators הגדרת

| Business Unit Objective | Measure | Target and Tolerance | Potential Event | Leading Indicator | Escalation Trigger for Business Unit |
|---|---|---|---|---|---|
| Develop product promotional campaign with supermarket chain in key region | Number of units sold per month per store | *Target*: 1,000 units of new product sold per month per store during promotional campaign *Tolerance*: 900–1,250 units sold per month per store | Consumer confidence decreases, resulting in decreases in purchases of the company's products | Consumer confidence indicators | Consumer confidence decreases by more than 5% |
| Create and maintain strong security against external intrusions on systems | Number of successful intrusions | *Target:* 0 per month *Tolerance*: 0 per month | Unauthorized individuals access the company's systems via Internet ports | Detected vulnerabilities in the company's core operating systems published by the vendor/third party; number of unauthorized attempts | New critical vulnerabilities identified by third parties |

# ניהול מאגר אירועים מבוסס מידע פנימי

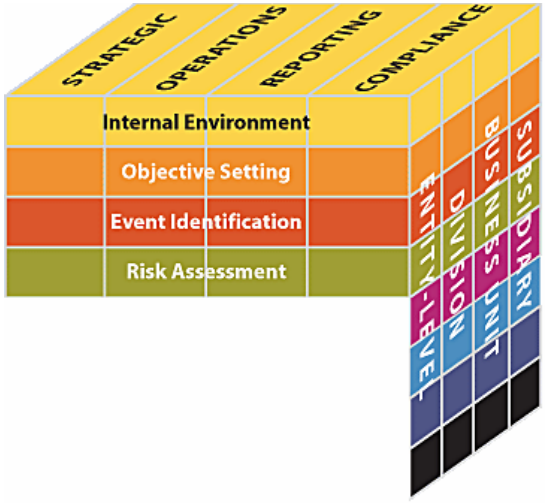
| Equipment | Component | Sub-component | Cause | Downtime Duration | Negative Effect on Production Availability | Cost |
|---|---|---|---|---|---|---|
| Pump #1 | Motor | Insulation | Overheating due to deterioration in insulation caused by excessive lead cable lengths | 1H: 20M | 0.4% | $24,000 |
| Pump #2 | Motor | Switch | Product defect | 2H: 10M | 0.7% | $42,000 |
| Conveyor | Belting | Roller | Contamination in the ball oil | 4H: 45M | 1.6% | $95,000 |

# איחוד אירועים

| Factors | Economic | Population Health | Service Delivery | Human Resources | Technology | Natural Environment |
|---|---|---|---|---|---|---|
| Events | Changes in | | | | | |
| | • Funding<br>• Exchange rates<br>• Interest rate<br>• Credit defaults<br>• Long-term capital availability | • Lifestyle choices<br>• Social behaviors<br>• Industry standards | • Acute intervention guidelines<br>• Ambulatory practices<br>• Continuing care practices<br>• Diagnostic procedures<br>• Disease prevention<br>• Emergency services practices<br>• Palliative care practices | • Employment opportunities<br>• Staff retention rates<br>• Physician and nursing staffing levels<br>• Evaluation procedures<br>• Health and safety practices | • System / data access protocols<br>• Data and system availability<br>• Available technologies<br>• Systems (implemented or abandoned)<br>• Health records requirements | • Emissions / waste products created<br>• Natural disasters |

# הערכת סיכונים - תיאוריה

- הבן את עוצמת הסיכונים היכולים להשפיע על מטרות הארגון
- הערך את הסיכונים בשני מישורים
  - עוצמת הנזק הנגרמת לארגון בקרות האירוע (השלכה)
  - הסבירות לקרות האירוע (סבירות)
- כימות הסיכונים
  - כמותי
  - איכותי
  - מימד הזמן
- התייחס לרמות הסיכון השונות



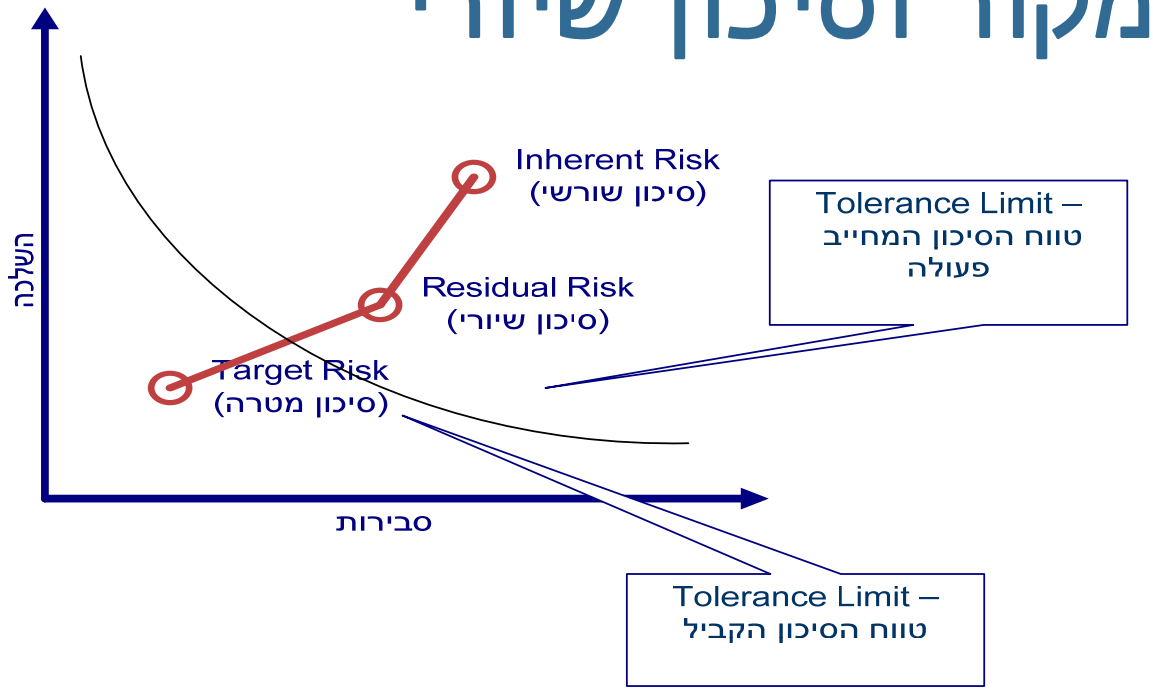
# הערכת סיכונים - פרקטיקה

- הבן כראוי את סיכון המקור והסיכון השיורי (לדוגמא: )
- עשה שימוש בסולמות הערכה:
  - איכותי
    - Nominal measurement – קיבוץ אירועים למשפחות (טכנולוגי, פיננסי)
    - Ordinal measurement – קיבוץ אירועים לפי סדר חשיבות (גבוה, נמוך...)
  - כמותי
    - Interval Measurement – שימוש בסולם מספרי בעל מרחקים קבועים מראש
    - Ratio Measurement – שימוש בסולם מספרי בו הערכים מצביעים על יחס בין מידת הנזק
    - Probabilistic Techniques (לרוב בשימוש לסיכונים פיננסים) – תפיסות הערכה מבוססות "at risk" כגון:
      - Earning at Risk ,Cash Flow at Risk ,Value at Risk
    - Non Probabilistic Techniques כגון:
      - ניתוח רגישות, ניתוח תרחישים, ניתוח stress

# הערכת סיכונים – פרקטיקה (המשך)

- המחש ויזואלית את הערכת הסיכונים
  - Heat Map –
  - Risk Maps –
  - הצגה מספרית –
- קבע תהליך מתודולוגי להערכת סיכונים ואמץ אותו לאורך כל התהליך. ראה דוגמא למתודולוגיות

# סיכון מקור וסיכון שיורי



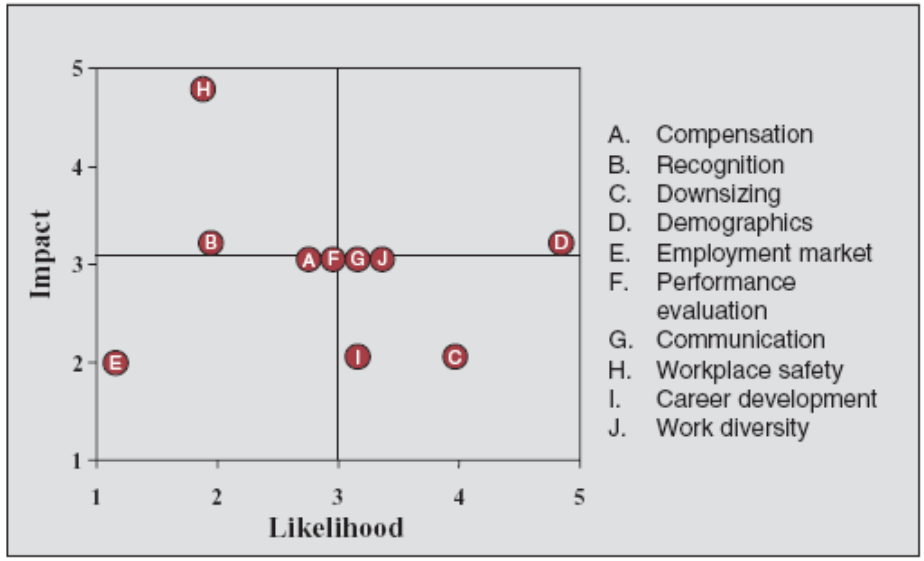

| Operations objective | Operating income from foreign operations of $100 million | | | | |
|---|---|---|---|---|---|
| Unit of measure | Change in operating income from foreign operations | | | | |
| Risk | Exchange rate fluctuation adversely affects operating income from foreign operations | | | | |
| Risk tolerance | Acceptable variation is +/- $10,000,000 | | | | |
| **Risk** | Inherent risk assessment | | Risk response | Residual risk assessment | |
| | Likelihood | Impact | | Likelihood | Impact |
| Foreign exchange rate moves up 1 percentage point within 90 days | 10% | $5,000,000 | No response in place | 10% | $5,000,000 |
| Foreign exchange rate moves up 1.5 percentage points within 90 days | 4% | $10,000,000 | Obtain foreign exchange hedge instruments to limit the impact | 4% | $5,000,000 |
| Foreign exchange rate moves up 3 percentage points within 90 days | 1% | $20,000,000 | | 1% | $8,000,000 |

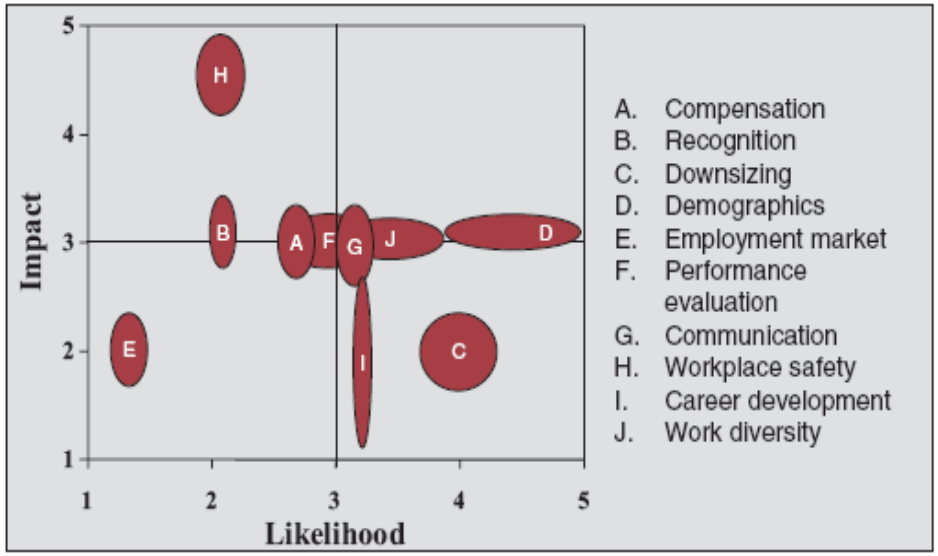
# Heat Map – המחשה ויזואלית

A company assesses risks to its objective of maintaining a quality workforce. Likelihood is considered in terms of percentage turnover within a specified period and impact in terms of cost of operational inefficiency and cost to replace, retrain, and develop employees. Color coding highlights those risks that are most likely to occur and most likely to have a significant effect on objectives.

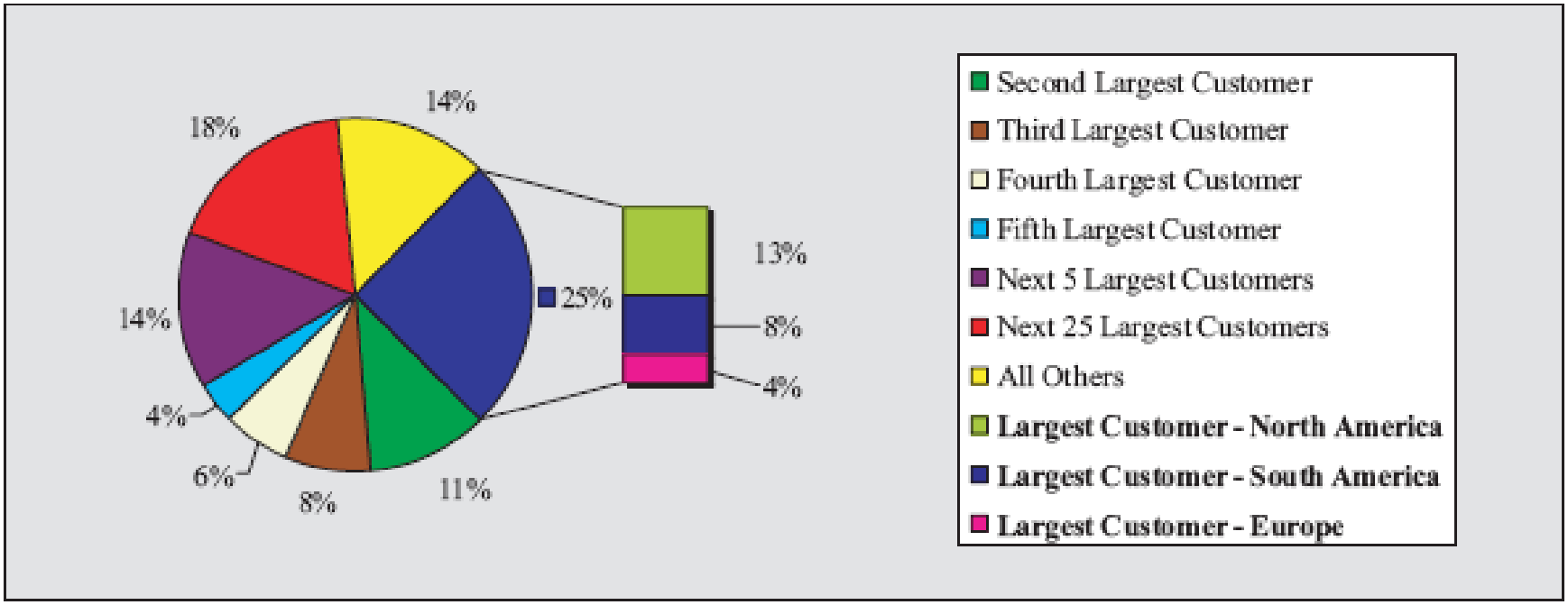
| | Topic | Risk Description | Likelihood | Impact |
|---|---|---|---|---|
| A | Compensation | Employee dissatisfaction with compensation leads to higher staff turnover. | Possible | Moderate |
| B | Recognition | Employees feel unrecognized, resulting in reduced focus on tasks and higher error rates. | Unlikely | Minor |
| C | Downsizing | Employees are over-utilized and work considerable overtime. Staff leave to pursue work in other organizations that offer a better work/life balance. | Likely | Moderate |
| D | Demographics | Changing demographic composition of the employee group causes increased turnover. | Almost Certain | Moderate |
| E | Employment market | Increased demand for company employees by recruiting firms. | Unlikely | Moderate |

# Risk Maps – המחשה ויזואלית

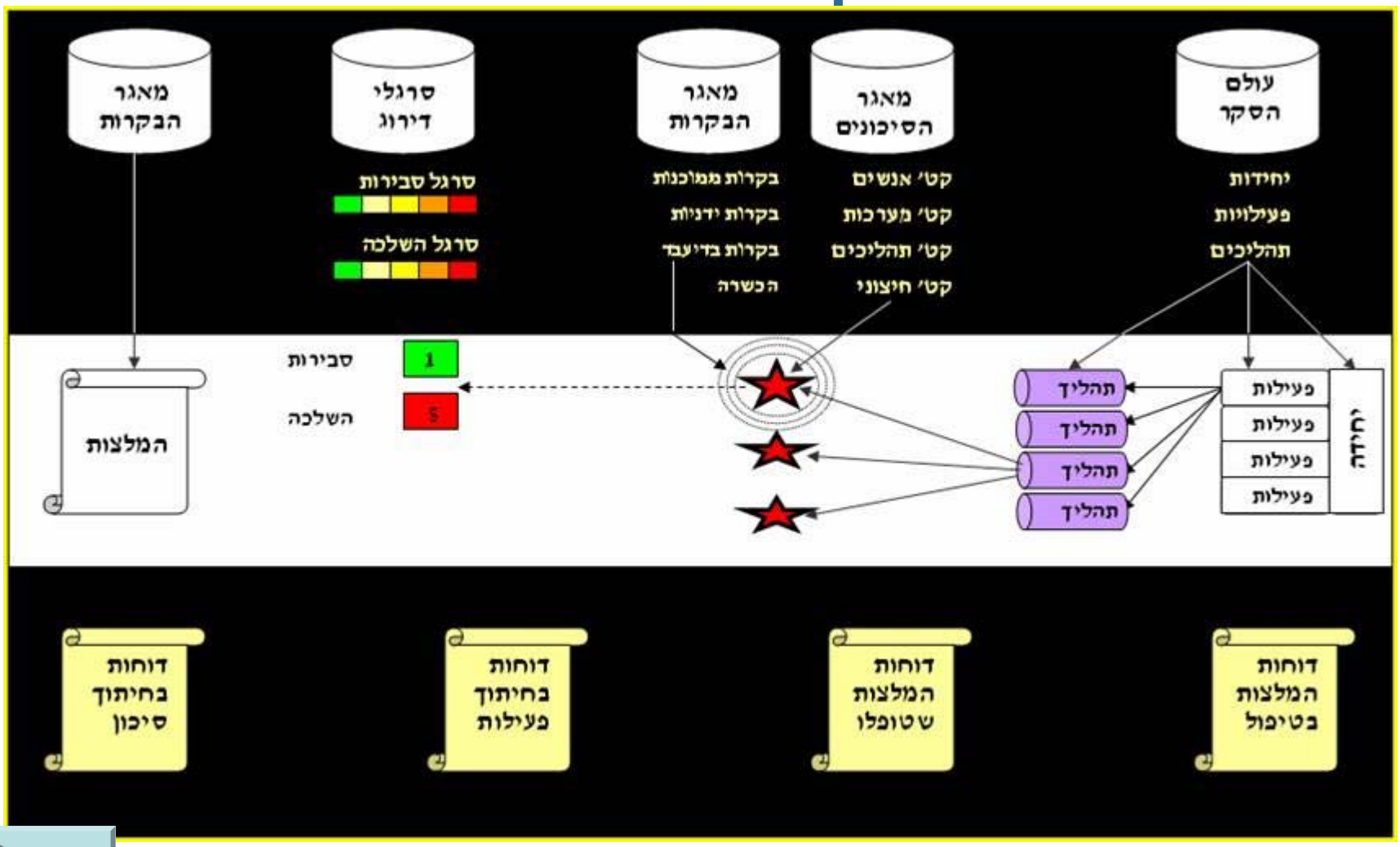


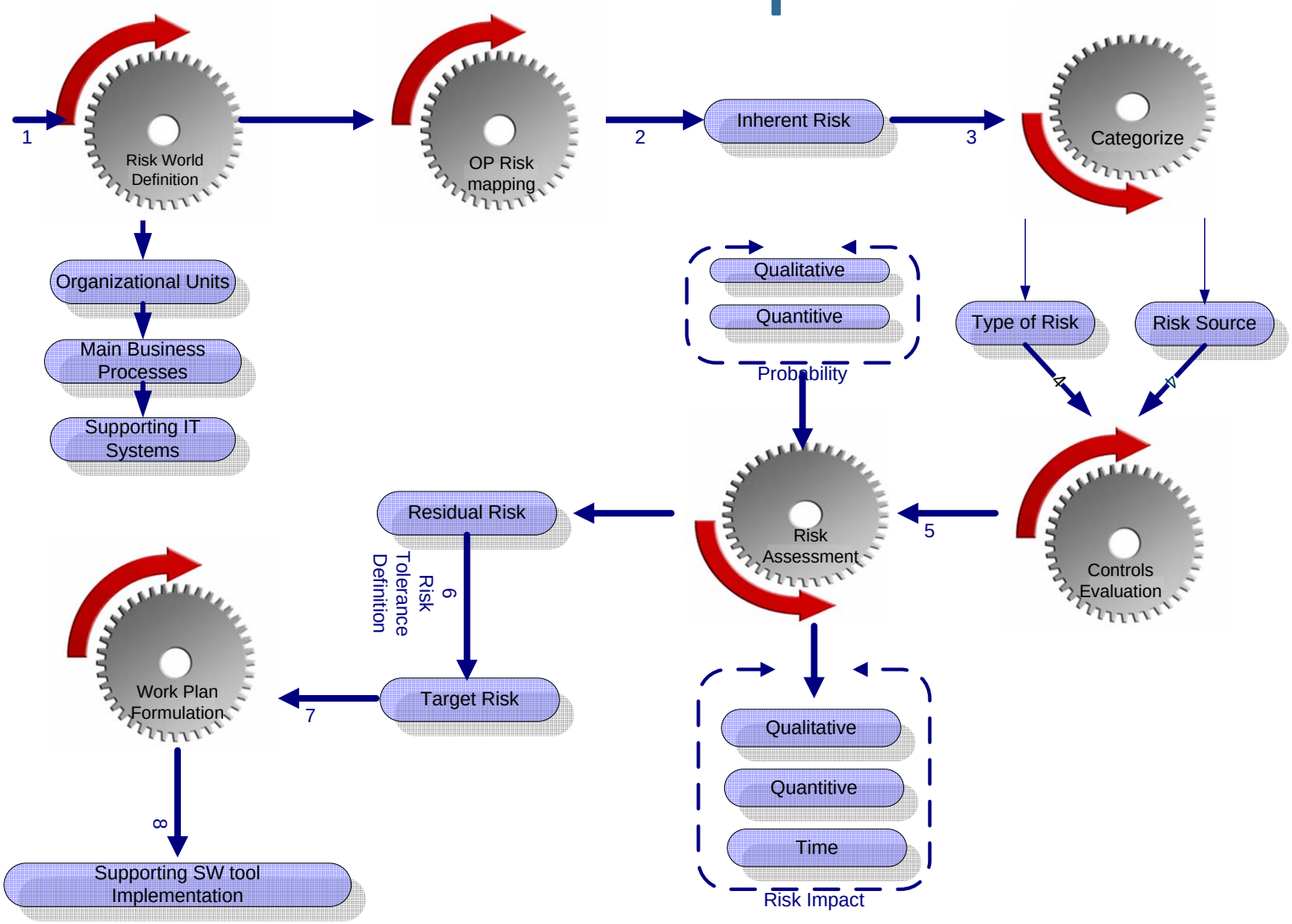
# המחשה ויזואלית – הצגת מספרית



# דוגמא 1 לתהליך מתודולוגיה

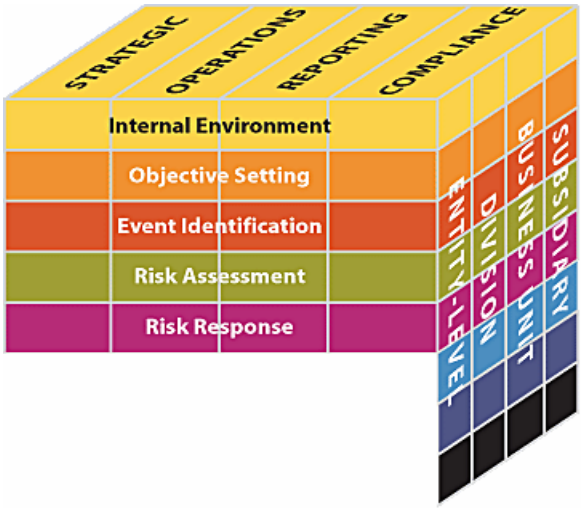


# דוגמא 2 לתהליך מתודולוגיה



# תגובה לסיכון - תיאוריה

- הגדר את תגובות הארגון לסיכונים השונים
- בצע הערכה של עלות \ תועלת בהקשר ל Risk Appetite
- קבע מה הוא המדד אותו יש להקטין (סבירות או השלכה או שניהם)
- עבור כל סיכון הגדר אחת מן התגובות הבאות:
  - הימנע – Avoid
  - מזער – Reduce
  - פזר – Share
  - קבל - Accept



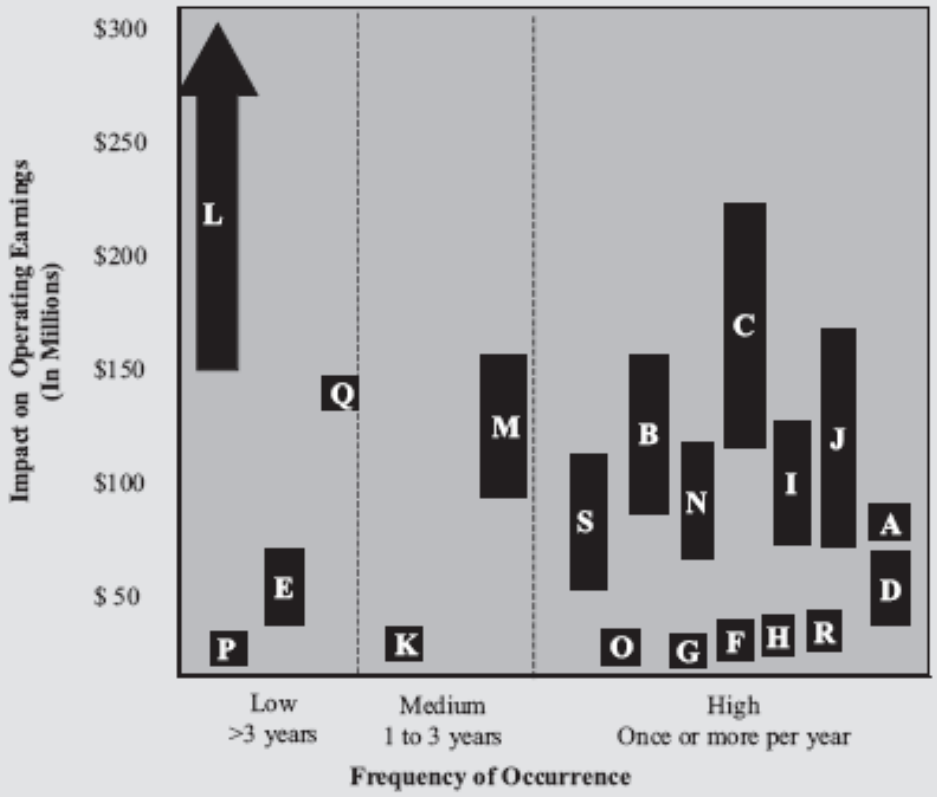
# תגובה לסיכון - פרקטיקה

- הגדר תתי תגובות לסוגי הסיכונים השונים
- קשר בין מטרות הארגון, אירועים, הערכת הסיכונים והתגובה לסיכונים
- בהתאם לסיכון ועוצמתו, שקול שימוש במספר סוגי תגובה לסיכון
- בנה מבט על ברמת יחידה וברמת הארגון על ה Residual Risk Profile

# ארבעת משפחות התגובה לסיכון

| Avoidance | Sharing |
|---|---|
| • Disposing of a business unit, product line, geographical segment<br>• Deciding not to engage in new initiatives/activities that would give rise to the risks | • Insuring significant unexpected loss<br>• Entering into joint venture/partnership<br>• Entering into syndication agreements<br>• Hedging risks through capital market instruments<br>• Outsourcing business processes<br>• Sharing risk through contractual agreements with customers, vendors, or other business partners |
| **Reduction** | **Acceptance** |
| • Diversifying product offerings<br>• Establishing operational limits<br>• Establishing effective business processes<br>• Enhancing management involvement in decision making, monitoring<br>• Rebalancing portfolio of assets to reduce exposure to certain types of losses<br>• Reallocating capital among operating units | • "Self-insuring" against loss<br>• Relying on natural offsets within a portfolio<br>• Accepting risk as already conforming to risk tolerances |

| Operations objective | • Hire 180 new qualified staff across all manufacturing divisions to meet customer demand without overstaffing<br>• Maintain 22% staff cost per dollar order | | | | |
|---|---|---|---|---|---|
| Objective unit of measure | Number of new qualified staff hired | | | | |
| **Tolerance** | 165–200 new qualified staff, with staff cost between 20% and 23% per dollar order | | | | |
| **Risks** | **Inherent risk assessment** | | **Risk response** | **Residual risk assessment** | |
| | **Likelihood** | **Impact** | | **Likelihood** | **Impact** |
| Decreasing number of qualified candidates available | 20% | 10% reduction in hiring → 18 unfilled positions | Contract in place with a third party hiring agency to source candidates | 10% | 10% reduction in hiring → 18 unfilled positions |
| Unacceptable variability in our hiring process | 30% | 5% reduction in hiring due to poor candidate screenings → 9 unfilled positions | Review of hiring process conducted every two years | 20% | 2% reduction in hiring due to poor candidate screenings → 4 unfilled positions |
| Alignment with risk tolerance | Response expected to bring company within risk tolerance | | | | |



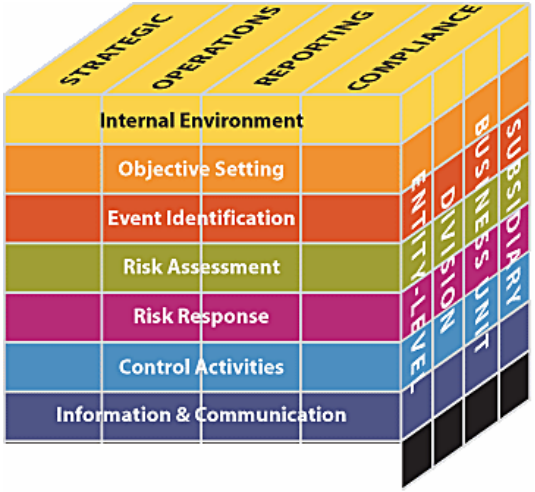

| *Event Category* | |
|---|---|
| A | Access to capital: Insufficient funds available to business unit |
| B | Supplier effectiveness: Supplier fails to deliver on commitments |
| C | Process efficiency: While effective, processes are too complex or manual to be in top tier when compared to leading practices |
| D | Process effectiveness: Processes are not as effective, resulting in defective outputs |
| E | Litigation: Risk of recall and class action lawsuits |
| F | Asset management |
| G | Demand: Inability to meet consumer demand |
| H | Intellectual property: Impact of patent infringements or R&D leaks |
| I | Leadership: Right people to drive business and efficient decisions |
| J | Governance: Sarbanes-Oxley, ethics & government compliance |
| K | Systems: Upgrades, enhancements |
| L | Concentration: Effectiveness of concentrations (e.g. customers, product categories, geographies, etc…) |
| M | Competition: New low cost competitors |
| N | Interdependencies: Between BU's |
| O | Economic |
| P | Employee Safety |
| Q | Government regulations |
| R | Employee capabilities: Skills, Losing key employees |
| S | Data confidentiality |

# פעילויות בקרה – תיאוריה ופרקטיקה

- הגדר נהלים ומדיניות לטובת הגדרת בקרות למזעור הסיכונים
- הגדרת בקרות כלליות (General Controls)
- הגדרת בקרות אפליקטיביות ( Applicative Controls)
- נדרשת הטמעה בכל רובדי הארגון
- הגדר את הבקרות כך שישמשו בתגובה לסיכונים

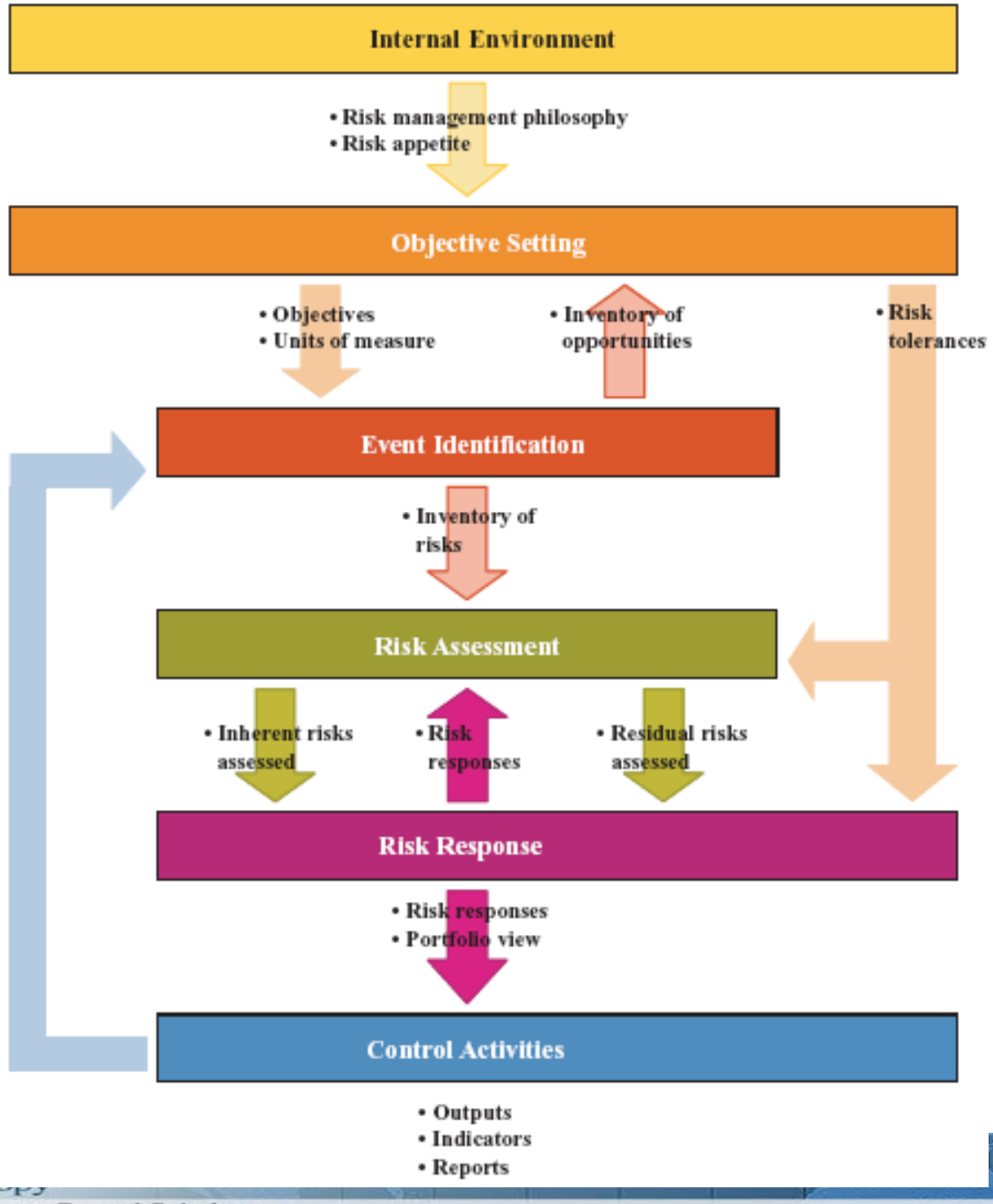
# מידע ותקשורת – תיאוריה

- שדר לארגון ולעובדיו את המידע הרלוונטי בפרקי הזמן הנכונים
- אין ליצור היצף מידע
- המידע והתקשור חייב להיות חוצה ארגון



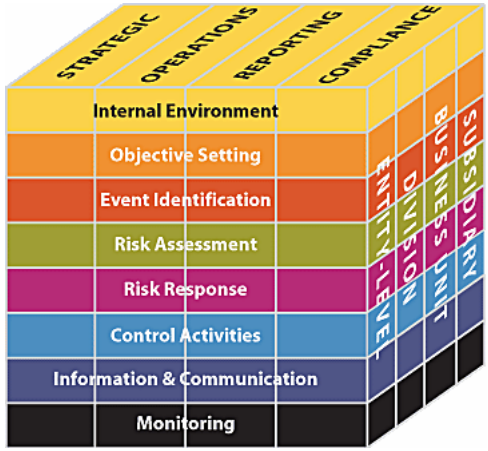
# מידע ותקשורת – פרקטיקה

- נצל את מערכות המידע של הארגון לטובת איסוף מידע
- שלב את מערכות המידע בתהליך בניית פרקטיקת ניהול הסיכונים
- עשה שימוש במערכות מידע תומכות המאפשרות
  - מבט על (Dashboard) של כל סיכונים הארגון
  - אפשר ביצוע Drill Down לסיכונים תפעוליים ולכל סיכון מנוטר
- נצל את ערוצי התקשורת של הארגון לטובת העברת מסרים (עיתון הארגון, דואר, email, פוסטרים ועוד)
- הקם אתר Intranet
- אפשר מעבר מידע בכל תהליך ניהול הסיכונים


Internal Environment
• Risk management philosophy
• Risk appetite
Objective Setting
• Objectives
• Units of measure
• Inventory of opportunities
• Risk tolerances
Event Identification
• Inventory of risks
Risk Assessment
• Inherent risks assessed
• Risk responses
• Residual risks assessed
Risk Response
• Risk responses
• Portfolio view
Control Activities
• Outputs
• Indicators
• Reports

# ניטור – תיאוריה

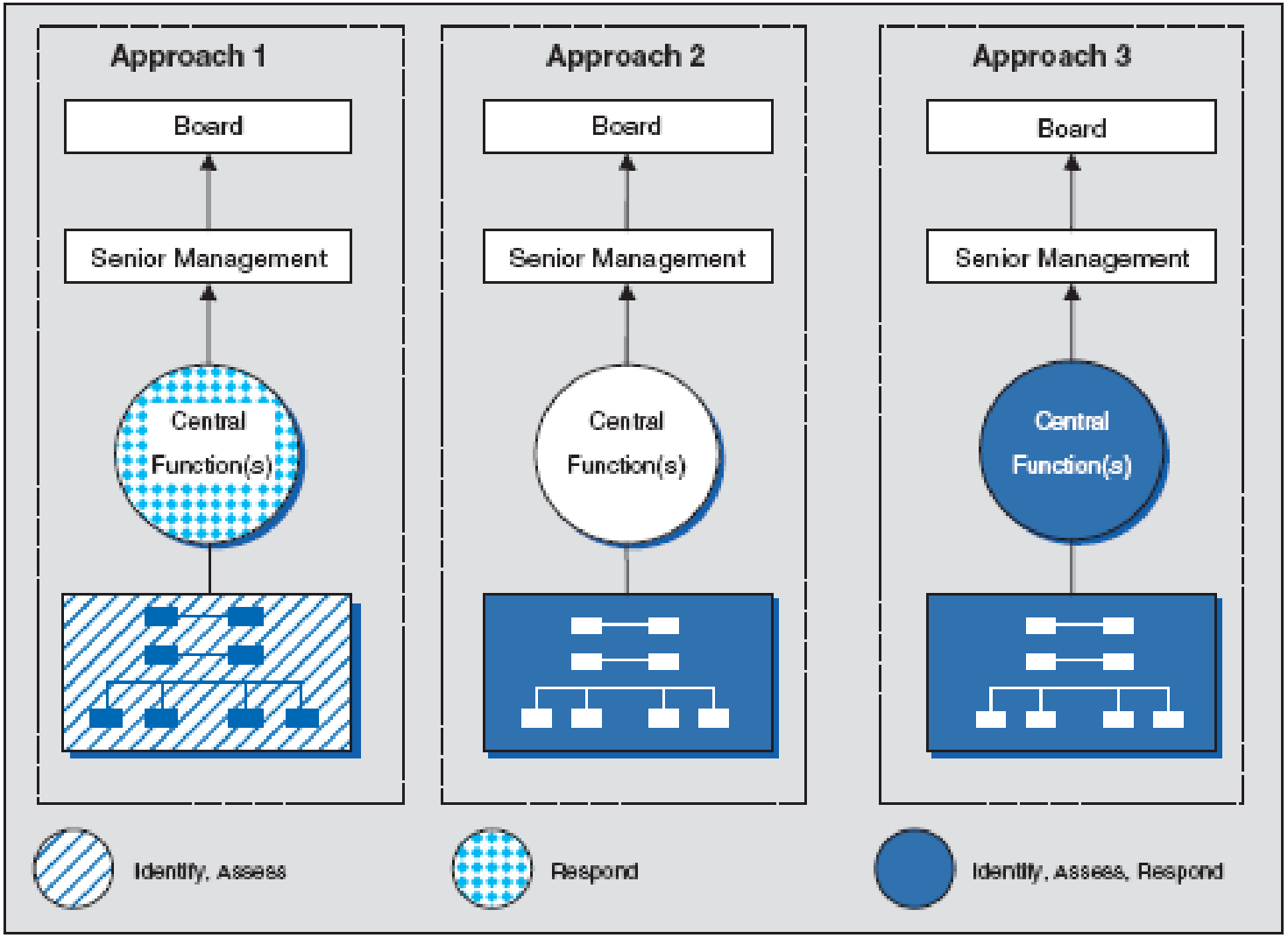
- יעילות תהליך ניהול סיכונים יתבטא, בין היתר ב:
  - פעילויות ניטור על בסיס קבוע
  - ביצוע הערכות של סיכונים בלתי תלויות
  - שילוב של השניים (בנפרד ויחדיו)



# ניטור – פרקטיקה

- הגדר מנגנוני דיווח ומערך דוחות המספק תמונת מצב טובה לגבי הסיכונים המרכזיים
- בצע סקרים והערכות סיכונים על כל מחלקות \ הקווים העסקיים של הארגון לטובת:
  - בחינה של יעילות תהליך ניהול הסיכונים
  - בחינה מחודשת של הסיכונים מזוויות מבט שונות
- שתף פעולה עם מחלקת הביקורת הפנימית לטובת שיתוף מידע
- תעד את כלל מערך ניהול הסיכונים של הארגון
- הגדר במפורש את כל תהליכי הדיווח הרלוונטים

# מבנה ארגוני תומך – דיון פתוח



# סוף

Questions ?