DCU Business School is proud to be home to the Emergency Management Institute Ireland (EMII). EMII is the primary professional organisation for individuals engaged in emergency and crisis management in the Republic of Ireland. Members operate in the professional, technical, voluntary and academic areas of emergency management.

The first Research Symposium explored risk management in Ireland, with particular emphasis on theory and practice in risk management at a national level (Government; Defence Forces; ESB). Four papers were presented:

- **Paper One:** Briefing on the MEM Framework (2018) Leonard, K.
- **Paper Three:** Risk Management in ESB. Sinnott, M., & Hynes, D.
- **Paper Four:** Defence Forces Approach to strategic risk. Mulcahy, R., & Lavin, D.

Papers from the EMII Research Symposium will be hosted on DORAS, DCU's Open Access Institutional Repository, in the hope that they can inform good practice in emergency management, while expanding the research database available to scholars and practitioners alike.
EMII Chairperson

Dennis Keeley

Chairperson EMII

Dennis Keeley is Assistant Chief Fire Officer in Dublin Fire Brigade. Dennis has also extensive international experience in Emergency Management. He was mobilised by the United Nations Disaster Assessment & Coordination (UNDAC) to assist with the management of international disasters in Pakistan and Ukraine.

Dennis is also a trainer and coach at the EU Civil Protection Mechanism Training Programme.
Paper One: Briefing
The MEM Framework (2018)

Keith Leonard
National Directorate for Fire & Emergency Management

Join @ www.emii.ie
Scope

• NSG approved a decision to review the existing Framework (22 September 2016)
• The aim of the review is to examine the structure and content of Framework (2006) and update the text to reflect the experience of the PRAs and other key stakeholders
Objectives

- Review Framework structure & content in light of the existing Framework after 10 years
- Reflect on doctrine and underpinning concepts
- Move some existing material to Guides & Protocols
- Link to work at national level
- Drive some new concepts / address issues that have arisen
- Holding with existing strengths
Purpose of the Framework 2006 - Context

- Provide a systems approach to emergency management from the risk identification stage, through the planning and preparedness stages to response and the recovery stage
- Ensure that each stage of emergency management is co-ordinated
- Define a common language & terminology
- Simplify inter-agency working
- Provide a system for assigning a Lead Agency in every emergency situation
The principles that underpin the Framework (2006)

• Protection and care of the public at times of vulnerability
• Clear leadership in time of crisis
• Early and appropriate response
• Efficient and co-ordinated operations
• Transparent and accountable system of emergency management
• Safe working
• Promoting community resilience
Areas identified for review

• Move emphasis from major emergencies to crisis management/management of normal emergencies wider use of co-ordination system
• Move some material to Guides & Protocols
• Emphasis on public communication
• Develop an approach to community resilience
• Build in community volunteers
• Align terminology with EU CP system – Civil Protection
• Link to national system
• Capture recovery process
• Health & Safety – policy for inter-agency aspect response
• Examine the requirement to develop enabling legislation
• Build in experience of Storm Ophelia and other recent events
Issues

- Legislation
- Prevention/ disaster reduction
- Public information
- Security
- Essential Services /CIP
- Technology/ Information systems
- Quality Assurance – Peer Review
- Resourcing & support
Programme

• Due to complete fist draft text November 2017
• Delayed due to Donegal flooding, Storm Ophelia and other LGD response
• Research & Development
  – DCU Lit. Review complete April 2017
  – Examine lessons identified from exercises & reports
• Workshop x 8 with RSGs
• Developing text – Project Team
• Aiming for 1st draft text by Q1 2018
Paper Two
Methodology, Process & Outcomes:
Delivering the National Risk Assessment 2017

Dr Caroline McMullan & Gavin D. Brown, DCU Business School
Eileen Tully, Department of Justice & Equality
Comdt Thomas Craven, Office of the Emergency Planning

Join @ www.emii.ie
Methodology, Process & Outcomes: Delivering the National Risk Assessment (2017)

Dr Caroline McMullan & Gavin D. Brown, DCU
Eileen Tully, Department of Justice & Equality
Comdt Thomas Craven, Office of the Emergency Planning
Previous Work

• National Risk Assessment 2012
  – Early stage assessment based on sound methodology from A ‘Framework’ for Major Emergency Management
  – First such assessment at national level
  – Accepted by EC as 'best in class'

• BUT time passes …

• Review & Update due for submission to EC
  – Opportunity to build on 2012 work and improve methodology
  – Greater alignment with international standard ISO 31000 desirable
  – Shortcomings in Impact criteria identified (fixed monetary values /casualty numbers). Relativity/Scalability needed
  – How to capture 'uncertainty'?
Methodology Must Be...

• Justifiable and appropriate to context
• Able to generate results which enhance understanding of the risks and how they can be treated
• Capable of use in a manner that is traceable, repeatable, verifiable
• Flexible enough to take inputs from different systems/departments/regions yet produce outputs that are comparable

(BS EN 31010:2010, p18)
At all times...

• Assessed on the basis of reasonable worst case scenario

• “The most serious credible outcomes/consequences”

(BS EN 31010:2010, p85/3)
Generation of the Initial Risk List

Data collected from:

• Regional Risk Registers
• Departmental Risk Registers
• National Agencies
Consolidated Risk List

• Initial assessment used to identify and screen risks quickly.
• Clustering of risks should be “consistent and defined at the start of the” process. (BS EN 31010:2010, p86)
• “Based on qualitative methods and summary information at a broad scale”. This will help ensure that lower priority risks do not have disproportionate amounts of time and effort expended on the assessment process. (Australian Guidelines)
• First output - Consolidated Risk List
<table>
<thead>
<tr>
<th>Hazard: Civil</th>
<th>Hazard: Natural</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Infectious Disease</td>
<td>1. Storm</td>
</tr>
<tr>
<td>2. Terrorist Incident</td>
<td>2. Flooding</td>
</tr>
<tr>
<td>3. CBRNe</td>
<td>3. Snow</td>
</tr>
<tr>
<td>4. Animal Disease</td>
<td>4. Low temperatures</td>
</tr>
<tr>
<td>5. Foodborne Outbreaks</td>
<td>5. High temperatures</td>
</tr>
<tr>
<td>7. Cyber Attack</td>
<td>7. Drought</td>
</tr>
<tr>
<td>8. Crowd Safety</td>
<td>8. Tsunami</td>
</tr>
<tr>
<td>10. Loss of Critical Infrastructure</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hazard: Transport</th>
<th>Hazard: Technological</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Road</td>
<td>1. Industrial Incident</td>
</tr>
<tr>
<td>2. Rail</td>
<td>2. Hazmat</td>
</tr>
<tr>
<td>3. Air</td>
<td>3. Fire</td>
</tr>
<tr>
<td>5. Transport Hub</td>
<td>5. Radiation Incident (Domestic)</td>
</tr>
<tr>
<td></td>
<td>6. Disruption to electricity/gas supply</td>
</tr>
<tr>
<td></td>
<td>7. Disruption to oil supply</td>
</tr>
<tr>
<td></td>
<td>8. Disruption to Communication systems</td>
</tr>
</tbody>
</table>
Risk Assessment

• “The goal … is to establish a standard and therefore comparable measurement of the likelihood and consequence of every identified hazard”. (Coppola, 2007, p.114)
Likelihood
## Likelihood Descriptors

<table>
<thead>
<tr>
<th>Rating</th>
<th>Classification</th>
<th>Average Recurrence Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Extremely Unlikely</td>
<td>500 or more years between occurrences</td>
</tr>
<tr>
<td>2</td>
<td>Very Unlikely</td>
<td>100 - 500 years between occurrences</td>
</tr>
<tr>
<td>3</td>
<td>Unlikely</td>
<td>10 - 100 years between occurrences</td>
</tr>
<tr>
<td>4</td>
<td>Likely</td>
<td>1 - 10 years between occurrences</td>
</tr>
<tr>
<td>5</td>
<td>Very Likely</td>
<td>Less than one year between occurrences</td>
</tr>
</tbody>
</table>

* For all but Terrorist Activity
Terrorist Activity – Likelihood

- Rating provided by the National Security Committee

1. Low – An attack is deemed unlikely.
2. Moderate – An attack is possible, but not likely.
3. Substantial – An attack is a strong possibility.
4. Severe – An attack is highly likely.

The threat is currently at moderate, upgraded from low last year.
Impact
<table>
<thead>
<tr>
<th>Impact Category</th>
<th>1 Very Low Impact</th>
<th>2 Low Impact</th>
<th>3 Moderate Impact</th>
<th>4 High Impact</th>
<th>5 Very High Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>People</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Deaths less than 1 in 250,000 people for population of interest OR Critical injuries/illness less than 1 in 250,000 OR Serious injuries less than 1 in 100,000 OR Minor injuries only</td>
<td>Deaths greater than 1 in 250,000 people for population of interest OR Critical injuries/illness greater than 1 in 250,000 OR Serious injuries greater than 1 in 100,000</td>
<td>Deaths greater than 1 in 100,000 people for population of interest OR Critical injuries/illness greater than 1 in 100,000 OR Serious injuries greater than 1 in 40,000</td>
<td>Deaths greater than 1 in 40,000 people for population of interest OR Critical injuries/illness greater than 1 in 40,000 OR Serious injuries greater than 1 in 20,000</td>
<td>Deaths greater than 1 in 20,000 people for population of interest OR Critical injuries/illness greater than 1 in 20,000</td>
</tr>
<tr>
<td><strong>Environment</strong></td>
<td>Simple, localised contamination.</td>
<td>Simple, regional contamination, effects of short duration</td>
<td>Heavy contamination localised effects or extended duration</td>
<td>Heavy contamination, widespread effects or extended duration.</td>
<td>Very heavy contamination, widespread effects of extended duration</td>
</tr>
<tr>
<td><strong>Economic</strong></td>
<td>Up to 1% of Annual Budget</td>
<td>Greater than 1% of Annual Budget</td>
<td>Greater than 2% of Annual Budget</td>
<td>Greater than 4% of Annual Budget</td>
<td>Greater than 8% of Annual Budget</td>
</tr>
<tr>
<td><strong>Social</strong></td>
<td>Limited disruption to community</td>
<td>Community functioning with considerable inconvenience</td>
<td>Community only partially functioning</td>
<td>Community functioning poorly</td>
<td>Community unable to function without significant support</td>
</tr>
</tbody>
</table>
Confidence Level
Confidence Level

• The goal is to capture the level of uncertainty present in the risk assessment
• Must capture this in order to interpret and communicate risk assessment results effectively (BS EN 31010:2010)

Refers to the:
• reliability, relevance and currency of the evidence/data
• input from appropriate experts
• level of agreement among assessors
# Confidence Levels

<table>
<thead>
<tr>
<th>Confidence Level</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>**High *****</td>
<td>Assessment based on expert knowledge of the issue and/or reliable, relevant, current data. Consistent agreement among assessors.</td>
</tr>
<tr>
<td>**Moderate **</td>
<td>Assessment informed by significant knowledge of the issue and/or limited reliable, relevant, current data. Broad agreement among assessors.</td>
</tr>
<tr>
<td>**Low ***</td>
<td>Assessment informed by limited knowledge of the issue and/or insufficient reliable, relevant, current data. Limited agreement among assessors.</td>
</tr>
</tbody>
</table>
6 x Focus Groups
Focus Groups

• Representatives from Government Departments and Agencies with the knowledge, experience and seniority to contribute effectively to the focus group discussions identified.

• All focus group participants received a copy of the agreed consolidated risk list.

• In advance each participant gathered relevant data and feedback in relation to the likelihood of the identified hazards triggering a national level emergency and the national impact of the reasonable worst case scenario.
Each focus group:

(1) Determined the likelihood of occurrence of each hazardous event on the basis of the reasonable worst case scenario

(2) Examined the current control/mitigation measures in place

(3) Estimated the impact of the hazardous event on people, the economy, the environment, and the social impact in accordance with the agreed national impact criteria

(4) Agreed the proposed risk score for each hazard.

(5) In accordance with the national confidence level descriptors, agreed the confidence level for each risk score.
Focus Group
3 Key Outputs

• Reasonable worst case scenario (RWC)
• Estimation of Risk
  – likelihood & impact of RCW*
• Confidence level for each risk assessment

* “the probability relevant to the selected consequence (RWC) is used and not the probability of the event as a whole” (BS EN 31010: 2010, p.85)
Threshold for Inclusion

- The aim of this NRA process is to determine the key national risks which require “a higher level of management” and to determine which risks “need not be considered further at this time” (BS EN 31010:2010 p.83).

- Risks rated as extremely or very unlikely and being of moderate impact or less and

- Risks rated as low or very low impact and which are considered to be unlikely to occur are not plotted on the 2017 National Risk Matrix.
National Risk Matrix 2017

Risk Assessment Confidence Levels:

*** High Confidence
** Moderate Confidence
* Low Confidence

A. Storm ***
B. Flooding ***
C. Snow ***
D. Low Temp. ***
E. Tsunami ***
F. Infectious Disease ***
G. Terrorist Incident ***
H. Animal Disease ***
I. Food Contamination ***
J. Loss of Critical Infrastructure ***
K. Rail Accident ***
L. Aviation Accident ***
M. Maritime Accident ***
N. Transport Hub ***
P. Hazmat **
Q. Fire ***
R. Nuclear Incident (Abroad) ***
S. Disruption to Energy Supply ***
T. Network & Information Security/Cyber Incident **

Impact vs Likelihood Matrix:

Very Low Impact

Very Likely

A. Storm ***
B. Flooding ***
C. Snow ***
D. Low Temp. ***
E. Tsunami ***
F. Infectious Disease ***
G. Terrorist Incident ***
H. Animal Disease ***
I. Food Contamination ***
J. Loss of Critical Infrastructure ***
K. Rail Accident ***
L. Aviation Accident ***
M. Maritime Accident ***
N. Transport Hub ***
O. Industrial Incident **
P. Hazmat **
Q. Fire ***
R. Nuclear Incident (Abroad) ***
S. Disruption to Energy Supply ***
T. Network & Information Security/Cyber Incident **

Very High Impact

Extremely Unlikely
Risks Below the Threshold for Inclusion

1. High Temperature ***
2. Volcanic Ash ***
3. Drought ***
4. Space Weather ***

5. Water Borne Outbreaks ***
6. Crowd Safety ***
7. Civil Disorder ***
8. Road Transport ***

9. Radiation (Domestic) ***

Risk Assessment Confidence Levels:

*** High Confidence
** Moderate Confidence
* Low Confidence
Expert Assessment vs Public Risk Perception

Household Preparedness Study 2017/18
NRA 2017

Flooding
Snow
Low Temperatures
High Temperatures
Storm
Drought
Tsunami
Fire
Loss Of Critical Infrastructure (E.G Water)

Infectious Disease (Humans)
Animal Disease
Nuclear Emergency
Terrorism
Cyber Incident

(Brown, McMullan, Largey, 2018, DCU Business School)
References

If citing this presentation, please use the following format:

Paper Three
Risk Management in Practice

Marie Sinnott & Derek Hynes ESB

Join @ www.emii.ie
Presentation to MSc in Emergency Management

Risk Management in ESB

Marie Sinnott
April, 2017
Agenda

• Introduction to ESB
• Oversight Arrangements
  • Roles & Responsibilities
• The Risk Management Process
• Group Risk Plan 2018
• Risk Appetite
• Business Continuity/Crisis Management
ESB Overview

- **Regulated Networks**
- **Generation**
- **Supply**
- **Innovation**

**ESB Networks**
- Owner of the Regulated Republic of Ireland T&D networks (2016 RAB €7.5bn)
- Owner of the Regulated Northern Ireland T&D networks (2016 RAB €1.6bn)

**NIE Networks**
- Portfolio 5.7 GW. All-Island Capacity 4.3GW and 47% Market Share. GB Capacity 1.4 GW
  - Diversified fuel mix. Capacity & Regulatory Supports

**Generation & Wholesale Markets**
- Diversified fuel mix. Capacity & Regulatory Supports

**Electric Ireland**
- 37% Market Share and 1.4 million Customers served on an All-Island basis

**History**
- Established 1927, Vertically Integrated, 95% Government-owned. Markets Ireland & UK

**Networks**
- Owner of the Regulated Republic of Ireland T&D networks (2016 RAB €7.5bn)
- Owner of the Regulated Northern Ireland T&D networks (2016 RAB €1.6bn)

**Generation**
- Portfolio 5.7 GW. All-Island Capacity 4.3GW and 47% Market Share. GB Capacity 1.4 GW
  - Diversified fuel mix. Capacity & Regulatory Supports

**Supply**
- 37% Market Share and 1.4 million Customers served on an All-Island basis

**Innovation**
- International Engineering consultancy; Telecoms, Smart energy services and E-Cars

**Financial**
- Regulated Networks Businesses account for ~ 66% of EBITDA and assets
- Solid EBITDA 2016 €1.32bn Assets €12.9bn Gearing 51%
- Strong Liquidity Position (2016 €1.7bn) and Stable Credit Ratings A-/Baa1/BBB+
Critical National Infrastructure Challenges

- **Impact of Climate Change**
  - More frequent extreme weather events
  - Increased flood risks

- **Increased reliance on technology**
  - Smart homes, appliances
  - Growing threat of cyber crime

- **Interdependence of networks**
  - Electricity/telecoms/water/gas

- **Customer Expectations**
Risk Oversight Arrangements in ESB
Risk Management in ESB

“... integrated business process essential to overall business success”

- Risk awareness
  - Example & tone set at the top – risks expected to be considered
  - Everyone has responsibility for risk
  - Consistency of language

- Decision making is informed by a proper analysis of risk
  - Strategy and Business Plans are the foundation
  - Framework for risk identification, assessment & escalation
  - In accordance with Risk Management Policy

- The risk framework is designed to support the culture
  - Our Values and Purpose
  - Framework practiced in a consistent manner across all business units
  - Oversight & accountability
# Risk Management Policy & Governance Framework

## Risk Management Framework

### Role of Board

- Approves Group Strategy
- Approves Risk Policy, overall Risk Management Framework, Risk Appetite, Risk Plans and performance targets

### Role of Board Committees

<table>
<thead>
<tr>
<th>Committee</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit &amp; Risk Committee</td>
<td>A&amp;RC advises on risk appetite, risk governance and other high-level risk related matters. Recommends Annual Risk Plan to Board.</td>
</tr>
<tr>
<td>Finance and Investment Committee</td>
<td>F&amp;I Committee advises on energy trading, treasury and investment/project related risk.</td>
</tr>
<tr>
<td>HSE Committee</td>
<td>HSE Committee advises on policies and procedures to ensure we meet our health, safety and environmental obligations.</td>
</tr>
<tr>
<td>Marketing, Customer &amp; Brand Committee</td>
<td>RemCo ensures alignment between approved risk appetite, compensation, selection and decision-making processes.</td>
</tr>
</tbody>
</table>

### Role of Senior Management

- Formulate and implement strategy within risk appetite. Responsible for risk governance and controls.
- Describes risks we are prepared to accept based on long term strategy, core risk principles, our values and risk management competencies

### Risk Appetite

- Our risk governance framework ensures appropriate oversight of and accountability for management of risk
- Our risk culture empowers our people to do the right thing for our shareholders, customers and staff.
- Our ‘Three line of defence’ model defines roles and responsibilities for risk management.
- An independent Risk Function ensures the necessary review and monitoring of risk.

### Risk Governance Framework

- Three lines of defence model

### Process

- People
- Independent Risk Function
- Risk management processes and procedures
  - Top and Emerging Risks
  - Risk & Control Heat Map
  - Business Continuity Testing
- Principal Business Unit Risks

### Underpinned by ESB Values

- Practices to identify, assess, monitor and mitigate risks that exceed our risk appetite
- Risks arising from our business activities that are measured, monitored and managed
Role of the Board and Chief Executive

• Oversight of the Risk Management Framework
  – Is Strategy and Risk aligned?
  – Are the right policies, plans, resources in place?
  – Are they lived and implemented?
  – Do we have the right culture to address risk in the business?

• Strategic oversight and guidance during a crisis
  – Manage the crisis professionally
  – Establish immediate response strategies and tactics
  – Manage communication with stakeholders
  – Protect ESB’s reputation
Culture – Questions for the Board

• **Is there an open and trusting relationship with the Chief Executive and the Senior Management Team?**
  – Is there a free flow of information sharing? Is the Board always kept informed?
  – Healthy challenge and debate?
  – A “no surprises” culture?

• **What is the level of engagement across the organisation? Are staff motivated and loyal?**

• **Are roles and responsibilities well understood? How are decisions made under pressure?**

• **Are there strong external relationships and networks in place that will support and sustain the business during a crisis?**
  – Can we leverage brand and reputation during a crisis? Are we in credit?

• **Does the business practice what it preaches when it comes to risk management?**
## Audit & Risk Committee Oversight

<table>
<thead>
<tr>
<th>Action / Responsibility</th>
<th>Suggested Frequency</th>
<th>Meeting Month</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Responsibilities</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOR 6 (a) (g) Support the Board in carrying out the Board’s responsibilities for ensuring that risks are properly identified, assessed, reported and controlled including advising the Board in the consideration of the overall risk appetite, risk tolerance and risk strategy of ESB Group</td>
<td>Annually</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>TOR 6 (b) (i) Review and recommend for approval to the Board the risk policy and risk management plan of ESB Group</td>
<td>Annually</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>TOR 6 (b) (ii) Review the key risks of ESB Group and the adequacy of planned mitigation</td>
<td>Quarterly</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>TOR 6 (b) (iv) Review the arrangements for business continuity planning for ESB Group</td>
<td>Annually</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>TOR 6 (b) (v) Advise the Board on the need for periodic external review of the effectiveness of the risk management framework for ESB Group</td>
<td>Quarterly</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>TOR 6 (b) (vi) Ensure that the risk management function is adequately resourced and has appropriate standing within ESB Group</td>
<td>Quarterly</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>TOR 6 (b) (vii) Keep under review the adequacy and effectiveness of the ESB Group’s financial and non-financial controls</td>
<td>Annually</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>TOR 6 (b) (ix) Review and approve the statements on internal controls (IC) and risk management in the ESB Group Annual Report and in the financial statements of ESB Finance Limited</td>
<td>Annually</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Risk Appetite
## Risk Appetite

<table>
<thead>
<tr>
<th>Risk level</th>
<th>Unable to take risk</th>
<th>Higher willingness to take risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prudent Financial Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presence of Scale Across Value Chain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GTS of Scale (Ireland, Northern Ireland, GB)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Engaged and Agile Organisation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sustainable Innovation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Value, Ethics and Compliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart Reliable Networks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What is a Risk Appetite Statement

- Risk Appetite is a statement of the Board’s willingness to take risk/pursue opportunities to achieve strategic objectives
  - A Statement of Intent – informs strategy and is informed by strategy
  - Has multiple dimensions/aspects
  - Set boundaries to risk taking – stretch for opportunity seeking
  - An aid to decision making
  - Used in context of assessing our Principal Risks
ESB’s Strategic Objectives reflect an underlying strategic intent...

<table>
<thead>
<tr>
<th>Strategic Objectives</th>
<th>Underlying Strategic Intent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Put customers current and future needs at the heart of all our activities</td>
<td></td>
</tr>
<tr>
<td>Produce, connect and deliver clean, secure and affordable energy</td>
<td></td>
</tr>
<tr>
<td>Develop energy services to meet emerging market needs</td>
<td></td>
</tr>
<tr>
<td>Grow the business whilst maintaining ESB’s financial strength</td>
<td></td>
</tr>
<tr>
<td>Deliver a high performance culture that supports innovation and collaboration</td>
<td></td>
</tr>
</tbody>
</table>
## Principal Risks

<table>
<thead>
<tr>
<th>Link to Strategy</th>
<th>Risk Climate</th>
<th>Safety &amp; Environmental Risk</th>
<th>Financial Impact</th>
<th>Key Risk Indicators</th>
<th>Within Risk Tolerance</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td></td>
<td>Risk of serious injury or death to staff, contractors or the public or damage to the environment resulting from our operations</td>
<td></td>
<td></td>
<td>▲</td>
<td>ALL</td>
</tr>
</tbody>
</table>

### Risk / Opportunity

<table>
<thead>
<tr>
<th>Link to Strategy</th>
<th>Risk Climate</th>
<th>Risk / Opportunity</th>
<th>Financial Impact</th>
<th>Key Risk Indicators</th>
<th>Within Risk Tolerance</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>▲</td>
<td></td>
</tr>
</tbody>
</table>

### Risk of damage to brand or reputation

<table>
<thead>
<tr>
<th>Link to Strategy</th>
<th>Risk Climate</th>
<th>Safety &amp; Environmental Risk</th>
<th>Financial Impact</th>
<th>Key Risk Indicators</th>
<th>Within Risk Tolerance</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td></td>
<td>Risk of damage to brand or reputation</td>
<td></td>
<td></td>
<td>□</td>
<td>ALL</td>
</tr>
</tbody>
</table>
Increased Focus on Recovery

- Boards need to accept that there are no guarantees
- Recovery as important as prevention
<table>
<thead>
<tr>
<th>HILP</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environmental</td>
<td></td>
</tr>
<tr>
<td>Major environmental disaster e.g.</td>
<td></td>
</tr>
<tr>
<td>Material breach of financing facility</td>
<td></td>
</tr>
<tr>
<td>Pension Risk</td>
<td></td>
</tr>
<tr>
<td>Governance failure/Major Fraud/Rogue Trader</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HILP</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure</td>
<td></td>
</tr>
<tr>
<td>Sabotage / Terrorism / Major Explosion / Fire causing damage to critical plant/infrastructure</td>
<td></td>
</tr>
<tr>
<td>Significant Supply Chain Disruption / Third Party Dependency</td>
<td></td>
</tr>
<tr>
<td>Severe Weather Event</td>
<td></td>
</tr>
</tbody>
</table>
Business Continuity Planning and Crisis Management Framework
<table>
<thead>
<tr>
<th>Framework</th>
<th>Owned by</th>
<th>Plan Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health &amp; Safety Organisation</td>
<td>EMP (Emergency Management Plan)</td>
<td>One plan exists for each significant building which deals with the initial alert and response. For example in the case of fire, our focus is on safety, damage limitation and security.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PPRP (Pandemic Preparedness &amp; Response Plan)</td>
<td>A Group-level plan provides for ongoing monitoring of the threat level and for triggering appropriate responses in the event of a pandemic. More specific plans exist at BU levels which complement the Group PPRP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Critical Incident Management Plan</td>
<td>The requirements for managing critical incident situations affecting ESB staff, contractors and their families and to ensure that their needs are recognised and responded to in a timely and appropriate manner are set out in the ESB Group Policy for Critical Incident Management.</td>
<td></td>
</tr>
<tr>
<td>Business Continuity Framework &amp; Structures</td>
<td>WARP (Work Area Recovery Plan)</td>
<td>One plan exists for each significant building, which provides for alternative accommodation. The focus initially is on relocating staff working on key processes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BU BCPs (BU Business Continuity Plans)</td>
<td>Typically one plan exists for each identified key process. This outlines how the local business team would recover and/or continue the business with reference to other plans.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CMP (Crisis Management Plan)</td>
<td>A plan exists for each BU and for ESB Group; focus is on efficient information collection; communications (internal and external); high level decision making and overall Incident Management; provides for supports required in the event of serious injury or fatality.</td>
<td></td>
</tr>
<tr>
<td>CIO</td>
<td>ITS-DRP (ITS Disaster Recovery Plan)</td>
<td>One integrated plan, from ITS Group, exists for all of ESB covering system recovery on a prioritised, pre-agreed basis (Note: any locally managed systems are catered for in relevant BCPs).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ITS Cyber Security Incident Response Plan</td>
<td>A plan, from ITS Group, exists for managing the response in the event of a cybersecurity incident</td>
<td></td>
</tr>
</tbody>
</table>
Integrated Contingency Planning
Practice Makes Perfect

Crisis Simulation

Exercising: Walkthroughs, Accelerated Phases, Real-time Simulations, Capability & Confidence

Plan Walk Through, Facilitated discussion, Real-time, Real-time, Multi-Team Simulation, Accelerated phases, Accelerated phases

Time & Realism, Full-scale live event

Compliance, Capability, Confidence

Energy for generations
Corporate Crisis

Notification / Activation Criteria

- Safeguarding of human life or safety at risk?
- A pan-ESB issue?
- Exceeds capacity of BU to contain/manage?
- Damage or potential damage to the reputation of ESB?
- Contamination of the environment?
- Significant interruption to supply or business activities?
- Large scale negative Media interest / coverage?

Exercise of Judgement
Conclusion

● Leadership from the top is key
  – Plan
  – Prepare
  – Practice

● Speed of recovery

● Innovate to manage risk

● Expectations have never been higher

● Have you thought of what it would be like to have no electricity……
Storm Ophelia
ESB Networks Response
Derek Hynes
Operations Manager
Customers Impacted across the Country

At its peak 385,000 homes and businesses had no electricity

- South West: 224,000
- Dublin South and South East: 55,000
- Mid West: 59,000
- Dublin North/Dundalk: 36,000
- North West: 11,000

There were over 5,500 individual fault locations
It resulted in 11.7m Customer Hours Lost
<table>
<thead>
<tr>
<th>Warning Level</th>
<th>Wind Speed (Mean km/h)</th>
<th>Gust Speed (km/h)</th>
<th>ESB Networks Response</th>
<th>Duration (Days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>STATUS YELLOW - Be Aware</td>
<td>50 to 65</td>
<td>90 to 110</td>
<td>0 - 5,000 customers without electricity</td>
<td>0</td>
</tr>
<tr>
<td>YELLOW level weather alerts are for weather conditions that do not pose an immediate threat to people or assets.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STATUS ORANGE - Be Prepared</td>
<td>65 to 80</td>
<td>110 to 130</td>
<td>5,001 - 30,000 customers without electricity</td>
<td>1 to 3</td>
</tr>
<tr>
<td>ORANGE level weather warnings can potentially impact on people in the affected areas and implies that recipients should prepare them selves.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STATUS RED - Take Action</td>
<td>&gt;80</td>
<td>&gt;130</td>
<td>30,001 - 300,000 customers without electricity</td>
<td>3 to 10</td>
</tr>
<tr>
<td>RED level severe weather warnings implies that recipients take action to protect themselves and/or their assets.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Note: All values are approximate and may vary depending on specific conditions.
Before the storm…

Day -4: Thursday Forecasts

Met Éireann Advisory issued on Thursday afternoon:

A combination of a vigorous Atlantic weather system and the remnants of Hurricane Ophelia will pass close to Ireland on Monday, and has the potential to be a high-impact event in parts of the country. There is a lot of uncertainty as to the exact evolution and movement of this weather system during the coming four days, but storm-force winds, outbreaks of heavy rain, and very high seas are threatened. Met Éireann will maintain a close watch on the evolution and issue further advisories and warnings as these are warranted.

Day -3: 2pm on Friday - Emergency Plan Invoked

Saturday 14/10/17

Level Red for southwest & west (5 counties), orange for the rest of country.

Ex-hurricane Ophelia is expected to bring severe winds and stormy conditions on Monday. Mean wind speeds in excess of 80 km/h and gusts in excess of 130km/h are expected, potentially causing structural damage and disruption, with dangerous marine conditions due to high seas and potential flooding.

Day -2: ESB Networks Crisis Management Meetings

Saturday morning and evening (Request assistance from UK on Saturday 9am)

Day -1: 3pm Sunday

Networks Emergency Management Team Convene in Leopardstown
National Co-Ordination

- NECG convenes Sunday 15th 10am
- Closure of Schools
- Extension of Red Warning to entire country
- Safety and Information
- ESB is a leader in this area
Storm Ophelia

Weather warnings

Red (take action) 6am to 1am
Violent & destructive gusts in all areas. Potential risk to life.

Amber (be prepared) 3pm to 10pm
Very windy weather. Transport disrupted & power cuts likely.

Sources: National Hurricane Centre, Met Office, Met Eireann
Stormy Weather – During Ophelia

Monday 16th October – Day 0

Safety
- Public Safety
  - Stay Safe Stay Clear
  - Contact us
- Staff Safety
- Wait until the wind has passed

Information
- NECG meeting @10am/2pm/4pm
- Network Storm Co-ord group meet 8am/2pm/7pm
- NEWSAC Meeting 9am Requesting support from UK utilities
- Forecasted customer outage of 450k
- Damage Assessment and Prioritisation
- Signal intent for the rest of the week

Restoration
- First fault at 07:45 Ballincollig Co Cork
- No work during the storm - remote operations via the Control Centre - FPE
- Work commenced at approx. 4 pm
Unprecedented…

Storm Ophelia - Customer Outage Volume 16th October
AFTER THE STORM
<table>
<thead>
<tr>
<th>Date</th>
<th>Day</th>
<th>Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>15-Oct</td>
<td>1</td>
<td>Public Safety Preparedness</td>
</tr>
<tr>
<td>16-Oct</td>
<td>0</td>
<td>Public Safety Expectations</td>
</tr>
<tr>
<td>17-Oct</td>
<td>1</td>
<td>Public Safety Restoration Prioritisation</td>
</tr>
<tr>
<td>18-Oct</td>
<td>2</td>
<td>Public Safety Estimated Restoration Times</td>
</tr>
<tr>
<td>19-Oct</td>
<td>3</td>
<td>Public Safety Geographic Report</td>
</tr>
<tr>
<td>20-Oct</td>
<td>4</td>
<td>Public Safety Updated ERTs</td>
</tr>
</tbody>
</table>

**Powercheck Pageviews 20th Feb - 26th Feb 2017**

- **15-Oct**: 70,000 Pageviews
- **16-Oct**: 80,000 Pageviews
- **17-Oct**: 90,000 Pageviews
- **18-Oct**: 100,000 Pageviews
- **19-Oct**: 110,000 Pageviews
- **20-Oct**: 120,000 Pageviews

**Key Messages**:
- Public Safety Preparedness
- Public SafetyExpectations
- Public Safety Restoration Prioritisation
- Public Safety Estimated Restoration Times
- Public Safety Geographic Report
- Public Safety Updated ERTs

**Immediate Priorities**:
- Damage Assessment
- Stakeholder Information
- What will come tomorrow

**Additional Information**:
- Storm Brian
- PowerCheck Pageviews 20th Feb - 26th Feb 2017

**Graphs**:
- Pageviews over time
- Percentage changes
- Bar charts for specific dates
There have been 2 incidents in the last 24 hours—one involved a slip trip & fall from a hoist & the second involved an NT on a pole. We are concerned about fatigue and exhaustion. All managers & supervisors are instructed to stand down staff, contractors & international crews involved in storm restoration works first thing tomorrow morning for 15 minutes to discuss the safety brief & risks associated with completing tasks when fatigued.

IMPORTANT: If you see a fallen wire do not approach it, they are extremely dangerous. Report them on 1800 372 999.

#StaySafe #Opales #Brian
Falling timber caused this pole to lean to one side. While the timber was being cleared from around the leaning pole, from a hoist, the pole fell and narrowly missed the main body of the hoist. Upon inspection the pole was rotten beneath ground level.

Be Aware & look out for hazards before starting work!
Storm Ophelia - Customer Outage Volume

- 32 X 38kV circuit outage
- 2 X 110/38kV transformer
- 2 X 110kV transmission line
- 334 MV CBs open
- 69 FPE operations
- 7,000 LV Faults
## Mutual Aid

<table>
<thead>
<tr>
<th>Company</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIE</td>
<td>187</td>
</tr>
<tr>
<td>Northern PowerGrid</td>
<td>16</td>
</tr>
<tr>
<td>WPD</td>
<td>37</td>
</tr>
<tr>
<td>Manx</td>
<td>5</td>
</tr>
<tr>
<td>Scottish Power</td>
<td>20</td>
</tr>
<tr>
<td>UK Power Networks</td>
<td>24</td>
</tr>
<tr>
<td>Electricity North-West</td>
<td>38</td>
</tr>
<tr>
<td>ENEDIS (France)</td>
<td>27</td>
</tr>
<tr>
<td>Morrison Utility Services</td>
<td>15</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>359</strong></td>
</tr>
</tbody>
</table>
Shoulders of Giants

- **Resources**
  - Nothing gets done without people
  - Army
  - NEWSAC
  - Contractors
  - Organisation

- **Staff Safety and Welfare**
  - Mobile drying units
  - Daily Safety presentations & Safety Performance
  - Food for depots
  - Inductions in Training Centre
  - Safety Briefings & Warnings to Public about fallen wires
  - Stock of PPE
  - Materials Management

- **Emergency Management**
  - Responsibility splitting – stakeholder, operations, media, welfare, action log & lessons learned, resources, information, communications, customer, safety
  - Devolved Control & Splitting areas
  - Daily SMT conference calls + SMT experienced in weather events
  - Help, support and interest from other parts of ESB

- **Customer and Stakeholder Management**
  - Leixlip Contact Centre open early
  - Information management
  - Managing politicians
  - Regular media & stakeholder briefings

- **Media**
  - Extent of media interest

- **IT and Social Media**
  - New OMS
  - Data Analytics
  - Depot, Worksite & MPRN Apps
The Future
“ESB Networks innovating towards a sustainable future for our customers and Ireland”
Decarbonisation

Current Carbon Emissions

- Agriculture: 33%
- Transport: 19%
- Heat: 15%
- Electricity Generation: 19%
- Other (Non ETS): 6%
- Other (ETS): 8%
• Connection costs
• Capacity
• Reliability
• Convenience
• Ethics

• Taxation
• Manufacturer adoption
• Social acceptability
• Retrofits
THE MAIN POINTS

- Mean Temperatures will increase by 1-1.6°C by mid century
  - All seasons will be warmer
  - More ‘hot’ days, less frosts
  - Increased growing season length
  - More heatwaves, less cold spells

- A decrease in overall rainfall
  - Drier summer and spring seasons
  - More frequent days with heavy rain in winter and autumn

- A slight decrease in overall storm activity but an increase in the number of severe storms
Thank You
Paper Four

Defence Forces Approach to Strategic Risk

Lt. Col Rossa Mulcahy & Comdt. Dave Lavin
Defence Forces Ireland

Join @ www.emii.ie
Irish Defence Forces
Risk Management

“Excellence is never an accident. It is always the result of high intention, sincere effort, and intelligent execution; it represents the wise choice of many alternatives – choice, not chance, determines your destiny”

Aristotle

Lt Col Rossa Mulcahy
Introduction – Who we are and What we do
Risk Management (RM) Policy and Guidance Documents
Risk Culture Development
Defence Organisation RM – Strategic Context
Guiding Principles DF SRM Processes & Policy
Scope of the Defence Forces (DF) RM
RM for Operations
Summary
Questions?
Early 2000’s heightened awareness of RM.
The Public Sector and Defence Organisation was not immune to the changing landscape.
Increased governance and accountability were necessary.
Utilisation of guidance documents to support the ‘new’ RM frameworks.
Military defence of the State (armed aggression)
Multi-national peace support and humanitarian relief operations
Aid the civil power (Garda Síochána)
Maritime security (Fishery Protection)
Joint Taskforce on Drugs interdiction
Aid to Civil Authority (major emergencies)
Ministerial air transport service (MATS);
Ceremonial Services
Fulfil other tasks/supports to government depts. and agencies (contingency)
Policy Space

Public Sector

- Good Governance in the Public Sector 2014
- White Paper on Defence 2015
- Risk Management for Government Departments and Offices 2016
- ISO 31000 2009

DF Guidance

- GRO H &S Risk Management 1/2010
- A.O. 02-2013 – COS RM Policy
- GRO DF Risk Management 04/2013
- Defence Forces Strategy Statement 2017-2020
- Brigade / Unit RM policies
Reflect Private Sector developments....

1. Political risk context.
2. Changing Domestic and International demands and responses.
3. Risk language, methods and frameworks.
Guiding Principles
Strategic RM

- Informed by best governance and ISO 31000.
- Embed SRM within existing structures and processes.
- Based on best available information. Risk Management for Government Departments and Offices 2016
- SRM is organisationally inclusive.
- Strategic Risk assessments are informed by strategic business objectives.
- Operational and branch risk registers are aligned through the use of common terminology.
Risk Identification (annually or as required)

Risk Analysis & Evaluation (quarterly or as required)

Risk Treatments (monthly)

SMC

SRC

SRWG

FREQUENCY

MONTHLY

QUARTERLY & AS REQUIRED

MONTHLY
<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Rare</td>
</tr>
<tr>
<td>2</td>
<td>Low</td>
</tr>
<tr>
<td>3</td>
<td>Medium</td>
</tr>
<tr>
<td>4</td>
<td>High</td>
</tr>
<tr>
<td>5</td>
<td>Very high</td>
</tr>
</tbody>
</table>
## Risk Categorisation = Likelihood X Impact

**Green**; 0 – 8; On target - No additional action required.

**Amber**; 9 - 16; Problem identified - Action ongoing to resolve.  
(or Potential problem - no action taken, carefully monitored).

**Red**; 17-25; Remedial action required immediately.
'Risk Management is the term applied to a logical and systematic method of establishing the risk context, identifying, analysing, evaluating, treating, rectifying, monitoring and communicating risks associated with any activity, function, process or achievement of an objective in a way that will enable the Defence Forces to minimise losses and maximise opportunities'.
Purpose

- ‘Afford protection to the DF…and the public service at large’

Risk Management:

- ‘Logical and systematic method…will enable the DF to minimise losses and maximise opportunities’

Responsibilities

- A COS (SRC)
- DSPB (SRC & SRWG)
The Defence Forces continues to strive for an Effective Risk Management environment.

Uniqueness of military life.

Part and parcel of our daily jobs.

Continued collaboration with the Department of Defence.

“…choice, not chance, determines your destiny…”