

CANADEM

Integrated Risk Management Doctrines & Procedures

1. CANADEM has a **high tolerance for operational risks**

- Utility for UN, GoC and others, as CANADEM is willing to accept certain risks that they need to transfer.
- Successful management of substantial risk transferred from the UN, GoC and others has created a resilient organization confident in its Integrated Risk Management capacity.

2. CANADEM is fiscally cautious and **financially risk-adverse**

- A CANADEM financial management principle is that almost always it is expending taxpayers' funds, and thus has a public-sector fiscal responsibility to ensure sound financial management.
- Having never had core funding, CANADEM is reliant on project funding that can be quite variable, a further incentive to be financially risk-adverse.

3. CANADEM practices **Integrated Risk Management**:

- regularly assesses its current risk tolerance, e.g. the sufficiency of its operational reserve;
- identifies and quantifies risks, then effects risk mitigation measures;
- designates Primaries, activity teams, and organization-wide cohesion on how to identify and address risk;
- manages risks events so as to avoid or limit actual harm.

CANADEM's 3 Key Risk Sectors



Three Risk Analysis Factors

#1 Likelihood
of risk occurring
e.g. 50%, 2%, 00.1% ?

#2 Impact
if risk occurs
catastrophic to simply annoying?

Level of Risk = **Likelihood** x **Impact**
(part math and part intuition)

Level of Acceptable Risk

#3 Acceptability -comfort level
with risk by board & staff

STOP?
or
GO?



Risk Assessment Process



restart the risk mitigation process

Is Inherent Risk Acceptable?

NO

YES

?

Risk is so unlikely and of such minor impact that no risk mitigation is necessary

Risk increases or changes?

1. Identify risk mitigation

2. Develop risk mitigation

3. Implement risk mitigation

Accept Risk

Monitor and Review Risk

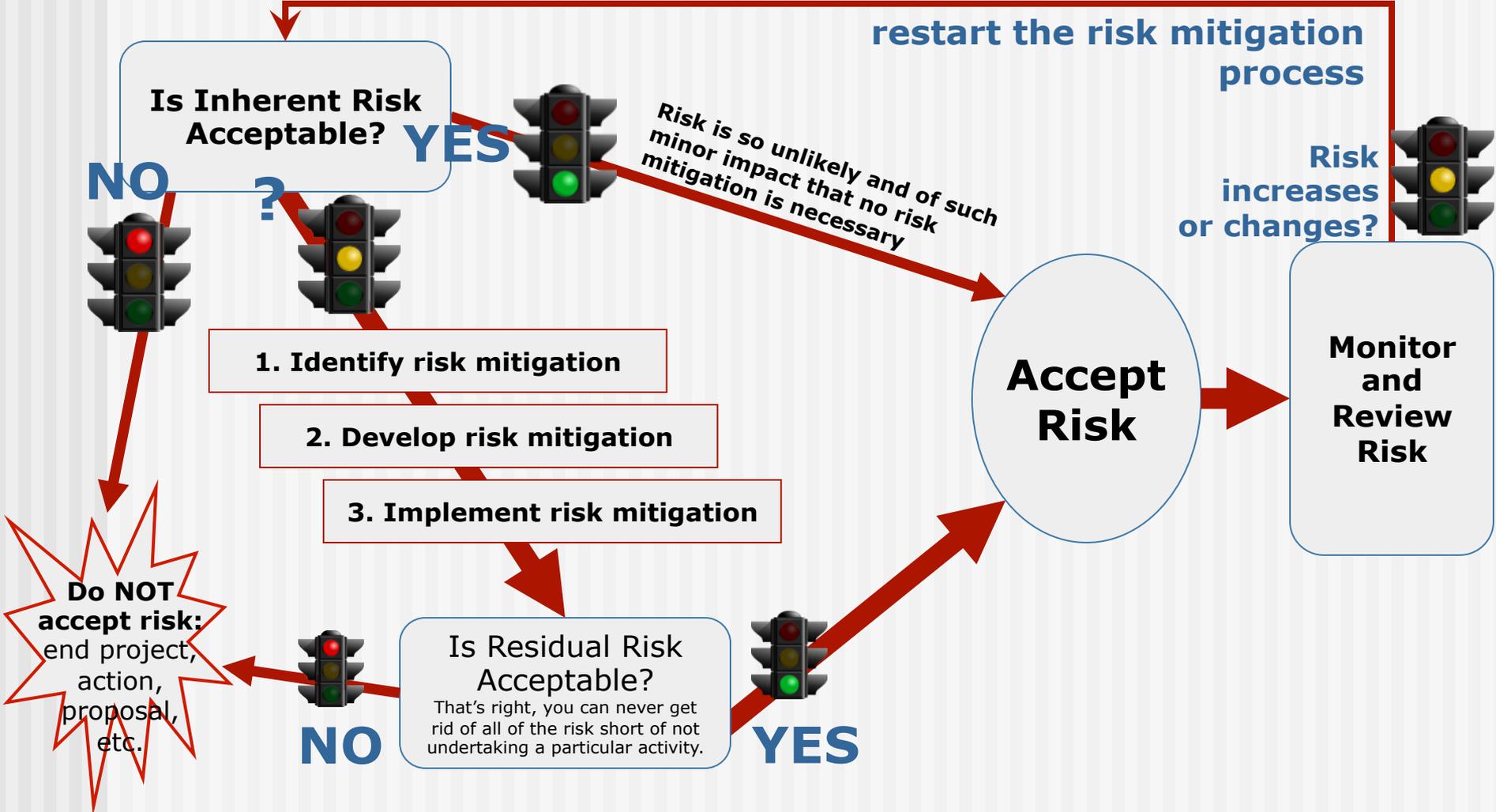
Do NOT accept risk: end project, action, proposal, etc.

Is Residual Risk Acceptable?

That's right, you can never get rid of all of the risk short of not undertaking a particular activity.

NO

YES



Integrated Risk Management (IRM) Informal Discussion Points

1. IRM procedures for the uninitiated can start to confuse, when in fact the basics are simple;
 2. These discussion points are designed for individuals coming new to IRM.
-

- There is no return without risk
 - Rewards go to those who take acceptable risks
- Communicate and ask questions
 - Search out & openly discuss risks
- Know what you don't know
 - Question your assumptions & adapt your actions
- Use common sense and avoid 'decidophobia'
 - Better to be roughly right than precisely wrong through inaction or a decision that is too late
- One for all, all for one
 - Only integrated teams achieve integrated risk management.

Some Risk Mitigation Measures or Approaches

- **Prevention:** e.g. stop or ban the activity
- **Reduction:** e.g. limit the activity
- **Redundancy:** e.g. back-ups, duplicate systems/equipment.
- **Controls:** e.g. multiple sign-offs, check-lists
- **Transfer:** e.g. by contract to transfer risk to consultants, insurers, etc.
- **Planning:** e.g. contingency plans, operations gaming
- **Financial Reserves:** e.g. ability to self-finance contingency actions
- **Training:** e.g. individuals and teams trained for what might happen

* **Risk Management is NOT the same as Crisis Management**

- ✓ This partial list of risk mitigation measures shows that **risk management** is systemic, constant, and a **normal** business activity. **risk**
- ✓ Only very occasionally will risk events escalate into crisis management. So having frequent crises indicates either particularly bad luck or ineffective risk management to avoid crises.

CANADEM a Resilient Organization

(based on staff capacity, not doctrine)

A key CANADEM value-added comes from being a resilient organization that

- ✓ adapts well to risk,
- ✓ learns from mistakes, and
- ✓ can be relied upon to *make it happen* when dealing with:
 - **External Risks:** high awareness of its operating environment, able to identify changes in external risks, and dynamically reinventing procedures and strategies;
 - **Unexpected Risks:** Withstand unexpected sudden change and instantly adapt;
 - **Internal Risks:** Internally networked and self-aware so as to rapidly detect new internal risks or errors, and take immediate corrective action.



WHY?

CANADEM's resilience in Integrated Risk Management comes from an empowered staff trained in 3 key CANADEM operational principles or attitudes:

1. **Subsidiarity Principle** of delegated authority
2. **Primaries** designated for all responsibilities
3. **Team Culture** including an *all-of-CANADEM 360° alert & support approach*, i.e. Integrated Risk Management.

Reason (HEAD) versus Feeling (GUT)

Some Psychological Risk Identification Mistakes

Read *Risk: The Science and Politics of Fear* by Dan Gardner

Calm informed analysis mitigates partial facts and/or intuition and/or emotion

Lack of hard data to quantify a risk does not mean there is no risk

Familiarity breeds contempt - won't happen to me.

Anchoring and Adjustment heuristic - we guess at level of risk using a recent number then adjust insufficiently

Availability Bias

"I remember a risk so it is more likely"

Some hard data does not mean that there is risk

"heard it on the news so it is more likely to happen"

A 'risk' is not a risk just because someone has a gut feeling

Group Polarization

AKA group think: people with same perspective when in a group become more convinced and less open to new info

Rule of typical things:

some details are plausible therefore the whole scenario is likely

Confirmation Bias

We hear what we want... to confirm what we already believe

Law of Similarity

Appearance equals reality ("it walks like a duck")

SMART DECISIONS

Remember other related CANADEM Procedures/Policies...

CANADEM Primaries

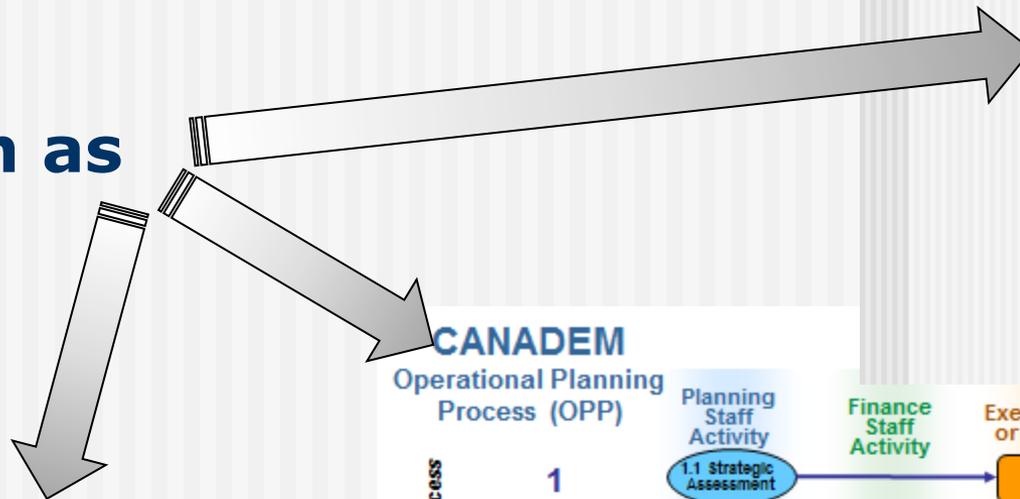
The use of Primaries is one of many organizational tools or operational procedures used within CANADEM.

This doc and those docs mentioned above are housed on the z-drive.

Updated July 2015

Please recommend changes/improvements as well as adding other examples of CANADEM in-house mapping. Send to Paul for inclusion on an updated version.

...such as



CANADEM Operations Gaming of activities and contingency plans

✓ Like a SWOT analysis, Operations Gaming is a heuristic technique to stress test a course of action (COA), ranging from intended activities to contingency plans.

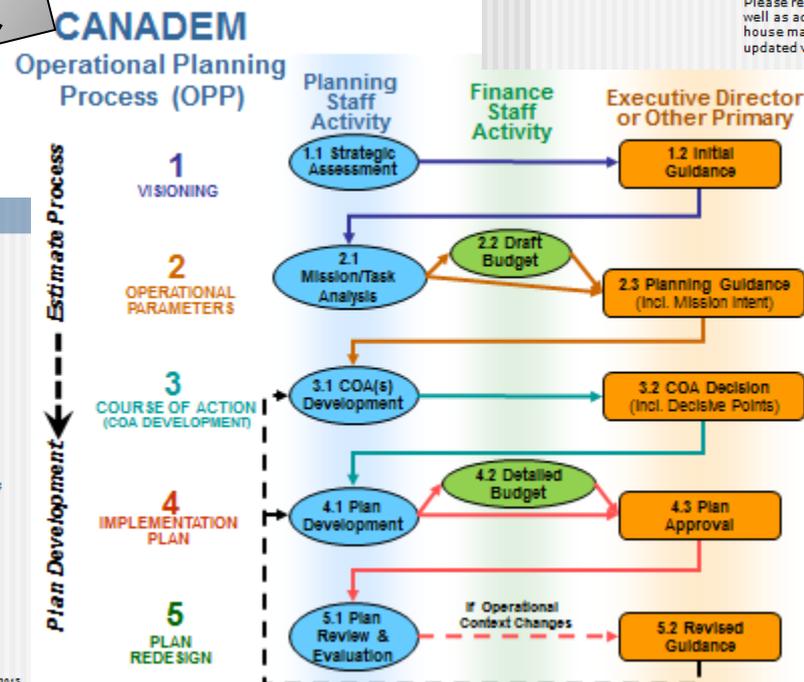
The aim is to assess:

1. if current risk mitigation measures, e.g. contingency plans, are sufficient
2. Identify risks not currently being considered

✓ PROCESS: in sequential stages following the COA timeline.

✓ PLAYERS: Usually two sides and a referee:

- ✦ The **Primary**(ies) planning to carry out a COA/mission/project at each stage will describe what they will achieve at that stage;
- ✦ **Disrupter**(s) who at each stage will respond and challenge assumptions and expectations with realistic risks ('what-ifs');
- ✦ A **Referee** will facilitate and arbitrate.



CANADEM Risk Management Roles & Responsibilities

- **Board:** Strategic direction on risk tolerance and risk management.
- **Executive Director**
 - Cultivate a **culture** of risk management, sensible risk taking, and team cohesion with *all-of-CANADEM 360° alert & support* as part of CANADEM's *Integrated Risk Management*;
 - Ensure **strategic** risks are identified, assessed, and managed;
 - **Operational** Risk – can delegate yet ED retains ultimate responsibility for all risks.
 - Provide guidance on operational risk management;
 - Engaged by Primaries as required for operational risk management.
- **Division/Unit Heads**
 - Ensure division/unit operational risks are identified, assessed, and managed;
 - Cultivate a culture of risk management, sensible risk taking, and team cohesion with *all-of-CANADEM 360° alert & support*.
- **All CANADEM Personnel**
 - Stay informed on risk management issues related to their operational piece;
 - Accept risk as part of daily business & take prompt action as risk materializes.
 - Understand and implement *all-of-CANADEM 360° alert and support*

All-of-CANADEM 360° alert & support

A core CANADEM operational principle that every individual is key to effective Integrated Risk Management (IRM). Regardless of position, every individual is key to mitigating every CANADEM risk by alerting others if they perceive risks, and supporting others to manage risks.

Model matrix with some example risk events

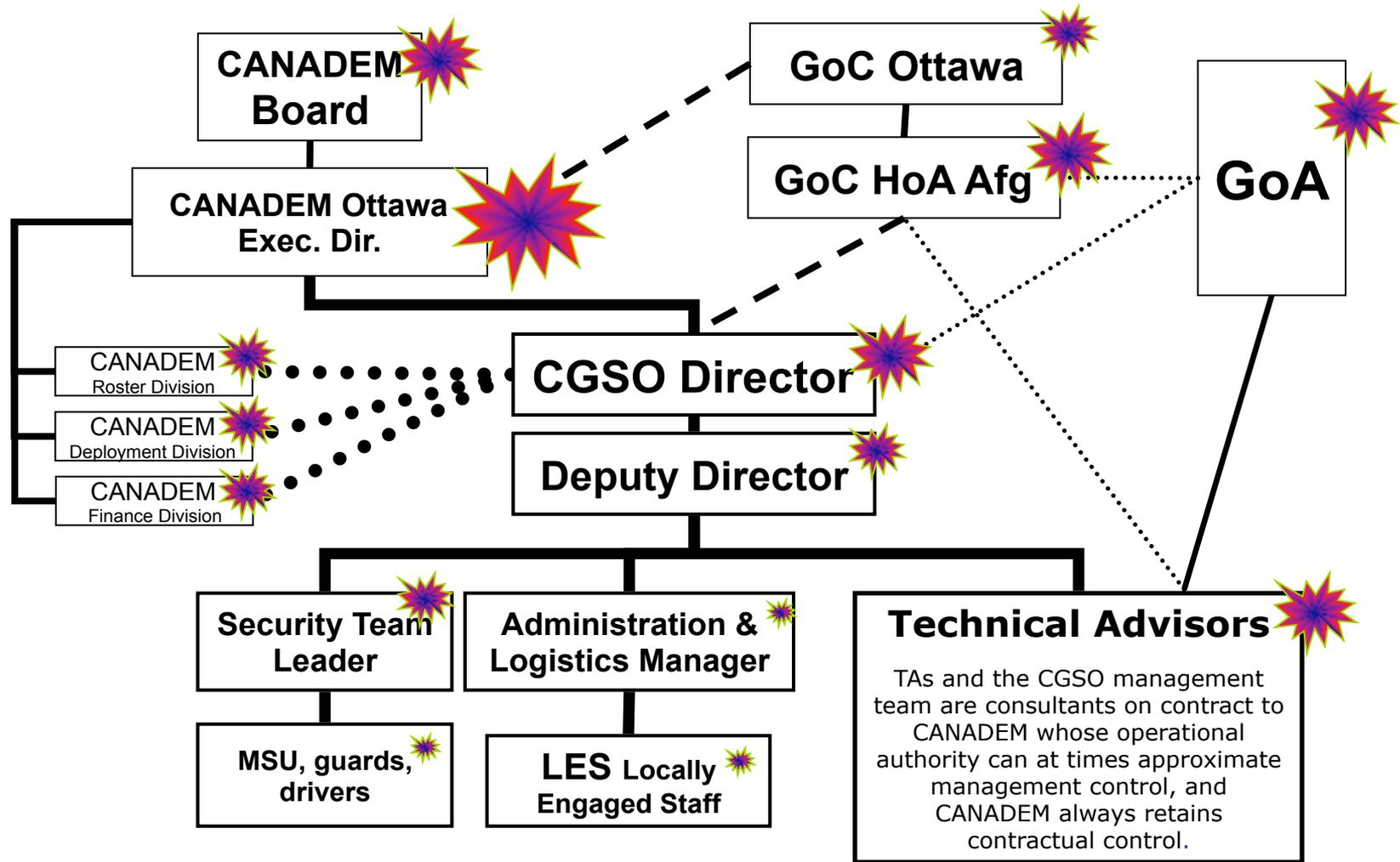
Risk Assessment Matrix

		IMPACT		
		Minor	Moderate	Major
PROBABILITY	Likely	moderate DFATD triggers advance work by CANADEM and then does not fund the project.	high	critical
	Possible	High maintenance deployee wastes our time low Deployee misses flight or loses money, e.g. pick pocket	High maintenance deployee wastes (UN) mission's time moderate Deployee mugged or in minor car accident	high Deployee killed or seriously injured
	Unlikely	low	Money transfer blocked or delayed low personal information files hacked	strong negative audit comments moderate Project substantially over budget

Liability & Limiting Liability

- Every organization and/or individual involved in an activity/project has liability of some sort, as determined by their:
 - ✓ Position or seniority;
 - ✓ Role or function; and
 - ✓ Reasonable expectation of their capacity and possible action.
- Liability can be partially limited through contractual relationships.
But courts are the final arbiter and will look to deny illegal or unfair liability-limitation by:
 - the more powerful in an unequal bargaining relationship; and/or
 - those in authority who should have been better informed, and who should have more effectively exercised their due diligence and duty of care.
- Liability can never be fully limited.
- Note that merely withdrawing from any activity will not avoid liability already incurred.

'Org Chart' of Relative Liability for CANADEM Deployed Personnel CANADEM-CGSO Afghanistan May 2010



- Operational authority (ranging from staff to consultants)
- Working link between CANADEM-HQ and CANADEM-CGSO
- - - - Strategic Oversight
- Coordination Linkages & Information Sharing

Always results in liability of some sort, albeit to varying degrees

Legal Liability

...can CANADEM be sued?

- So far not, but yes we can be sued.

The courts will decide if we have sufficiently met our duty of care.

They look at the actual events, but know that nobody can prevent every risk event, so the courts, barring laws or contracts* to the contrary, will apply the 'reasonable' person test:

Did CANADEM do everything that a '**reasonable**' individual/agency would do to mitigate '**reasonably**' likely events.

- Can CANADEM **prove** (e.g. document) that we:
 1. Identified all 'reasonably' likely risks, e.g. documented ops gaming; and
 2. Have we legally (contractually*) transferred certain risks, e.g. through insurance, or to sub-contractors including consultants; and
 3. For all remaining risks did we take 'reasonable' mitigating measures such as
 - a. Clear lines of authority & responsibility, with responsibilities set at the right level, e.g. subsidiarity and primaries;
 - b. Risk and security analyses both initially, and then regularly reviewed/updated
 - c. Resultant contingency plans and procedures (SOPs), also regularly reviewed/updated
 - d. Sufficient training & information sharing with/between:
 - All individuals so that they can mitigate risk
 - Key staff so that they can mitigate risk and ensure that others are mitigating theirs.

* Contracts can inadvertently create liability that is greater than the 'reasonable' test applied by courts, so concise contracts may well be better than complicated contracts.

Balancing risk management documentation against achieving other pressing tasks/goals

- CANADEM since 2002 has effected substantial operational risk management but without much documentation of that risk management. This has two key drivers:
 - Small team-minded staff where integrated risk management (IRM) is second nature;
 - Operational principles/practices such as *primaries* and *subsidiarity* that enable ad hoc risk management that is both sufficient and an optimum allocation of resources to fit the requirements of rapid response and tight budgets.
- So CANADEM is confident that its Integrated Risk Management is being achieved.
 - Management & other Primaries are aware of and managing key strategic & operational risks; carrying out a risk assessments before making important decisions.
 - All CANADEM staff have an understanding of CANADEM risk management doctrine. They are empowered to take smart decisions incurring risks, mitigate those risks, and know that they have the backing of management if risks materialize.
- But such confidence is a risk in itself, and since our risk management process is not substantively documented, perhaps CANADEM is deceiving itself?

One key mitigation is that CANADEM is self-aware of this risk of complacency and the need to further mitigate, e.g. IRM refresher training, or proactive ad hoc consideration of strategic and operational risk whenever there are key decisions or major events/trends

Risk-Communication

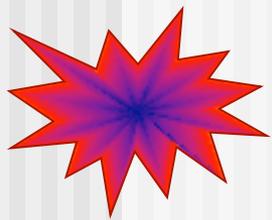
Risk-communication can increased internal and external confidence by showing that:

1. CANADEM has a sound IRM (Integrated Risk Management) system;
2. has identified risks properly;
3. understands those risks; and
4. is taking sufficient mitigation measures.

Some risk-communication Myths and Realities

MYTH*	REALITY
Talking about risk will only alarm others.	Experienced outsiders know there are risks, and if well communicated by CANADEM, they will be reassured.
Risk is too complicated to explain to others.	IRM is based on common sense, and by using common language not techno-babble, CANADEM can explain CANADEM risk management to the public and other stakeholders.
Risk communications is the job of the communications people	Every CANADEM individual is part of IRM and can speak to their area of risk awareness and risk management. They may be the best spokesperson albeit with assistance and direction from senior management and communications people in order to retain a coherent CANADEM response.

- * These myths stem from legitimate worries about risks inherent in any communications. But silence when there should be communication and transparency is a mistake. At the same time, like diplomacy, in some situations silence is the right risk mitigation.



Emergency! Crisis! Death?!

A Risk Event & CANADEM Response

Despite proper and sufficient risk prevention, bad things will happen, what is called a *risk event*.

1. All staff should be aware of our current response protocols
2. When a *risk event* occurs, staff should immediately look at those protocols

See: **2014-04 CANADEM HQ Critical Incident Response Immediate Procedure:**

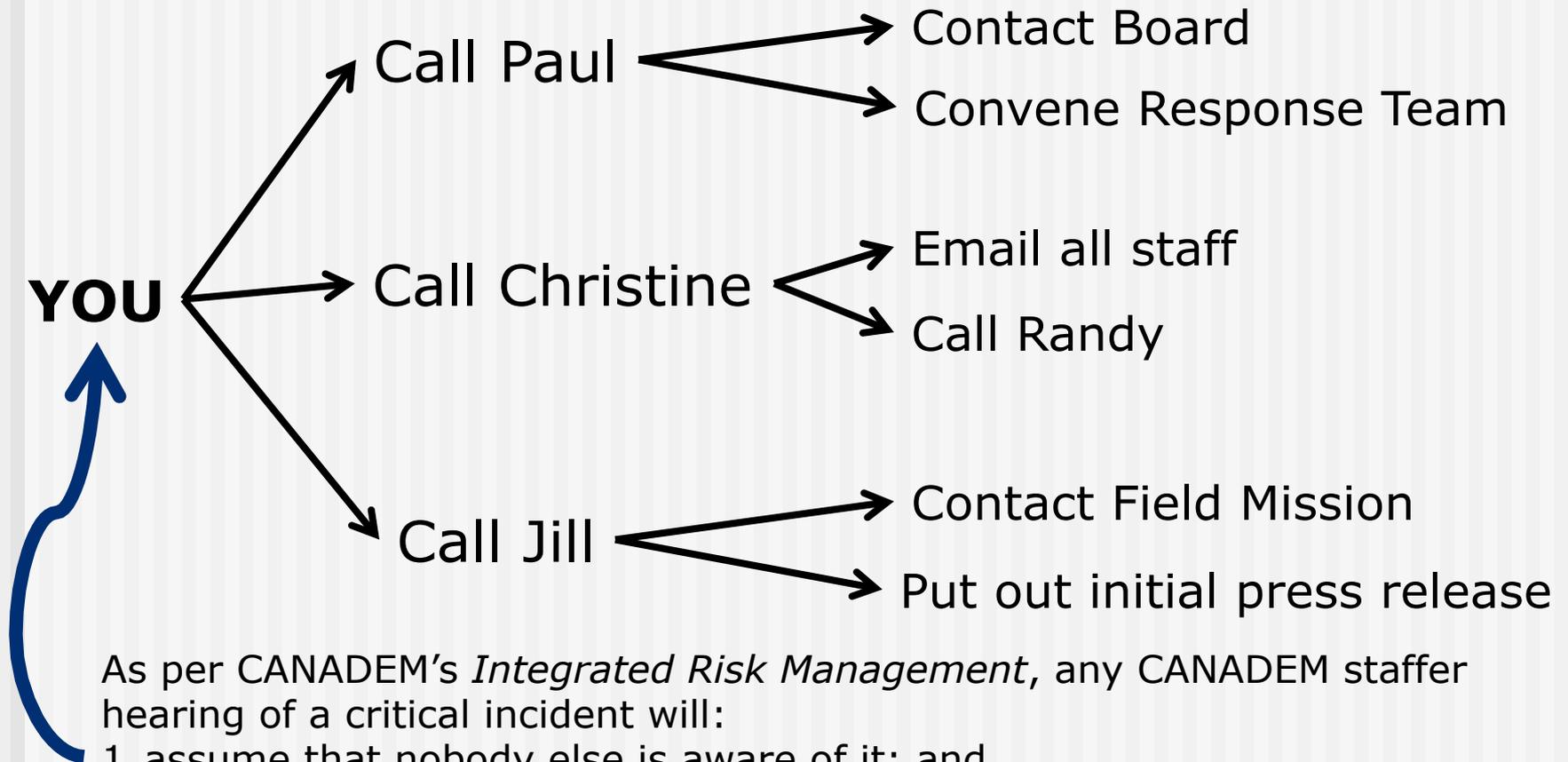
Z-drive/DOCTRINE and other core CANADEM Documents/2014-04 CANADEM HQ Critical Incident Response Procedure.doc

Throughout initial and subsequent actions, the principles in order of priority are:

- Best interests of the victim and their immediate family
- Concern about other CANADEM staff/associates in the field
- Advancing optimum CANADEM and/or mission mitigation measures
- Addressing CANADEM liabilities and risks
- Transparency with the media and public without infringing privacy issues.

CANADEM

Critical Incident Fan-Out



As per CANADEM's *Integrated Risk Management*, any CANADEM staffer hearing of a critical incident will:

1. assume that nobody else is aware of it; and
2. take the immediate initiative of calling Paul+Christine+Jill
(see CANADEM HQ Critical Incident Response Immediate Procedure on z-drive)

Note to non-CANADEM

- Of course, feel free to use this powerpoint, and adapt it for your use. We hope it is useful.
- Try watching it in **slide show** mode, as some slides have animations that you might find useful, and can easily go to the Animation Pane to build in pauses if you are training.
- CANADEM's in-house powerpoint is more extensive.
- If you are interested in contracting CANADEM to help you customize this presentation or provide training assistance, please contact
Paul.LaRose-Edwards@CANADEM.ca

END
