GOVERNMENT RISK MANAGEMENT

2015 ICGFM CONFERENCE
ABOUT MULTILATIN

**MultiLatin** helps companies mitigate risks associated with contracting of employees & business partners in Latin America & the Caribbean.

We do so in order to help:

- **Protect our client’s reputation**
- **Prevent fraud & corruption**
- **Strengthen security in workplaces**
- **Meet international compliance standards**
FREEBALANCE

Canadian Company

High Success Rate

GRP Leader

Modern Web Technology

100% Government Focus

Global PFM Provider

Covers Budget Cycle

ISO-9001/2008
APPROACH TO

Doug Hadden, Executive Vice President, Strategy and Innovation, FreeBalance
EXERCISES

• Multiple scenarios provided to groups
• Worksheets are included
• Feedback from groups
WORKSHOP AGENDA

• Introduction to Risk Management
• Reputational Risk & Exercise
• Risk and Public Financial Management Planning
• Problem of Risk Avoidance
• Risk Matrix & Exercise
• Governance, Risk & Compliance Software
• Planning Tools Integration
• IT Risk Management
• Risk Management Maturity & Exercise
• Using This with Your Government
WHY?
TECHNOLOGY ENABLED
INCREASED DEMAND FOR IMPROVED CITIZEN SERVICES
INCREASED PARTICIPATION
OLD SOLUTIONS
COMPLETE CHANGE IN RISK CALCULUS
RISK = INNOVATION
RISK = OUTCOMES
RISK = $$$$
BUSINESS AS USUAL
ASSUME
RISK IS ABOUT MITIGATION
RISK IS ABOUT PLANNING
& ANTICIPATING OUTCOME BENEFITS
PRACTICE OF RISK MANAGEMENT, NOT RISK IN DEVELOPMENT
THEMES

RISK  BENEFIT  MITIGATE

FreeBalance  MultiLatin
WORKSHOP AGENDA

• Introduction to Risk Management
• Reputational Risk & Exercise
• Risk and Public Financial Management Planning
• Problem of Risk Avoidance
• Risk Matrix & Exercise
• Governance, Risk & Compliance Software
• Planning Tools Integration
• IT Risk Management
• Risk Management Maturity & Exercise
• Using This with Your Government
Presentado por:

David Robillard, Managing Director
Reasons to Pull Out of a Negotiation

Have you pulled out of a deal because of any of the following?

- Lack of confidence in management: 82%
- Unquantifiable/unknown liabilities: 52%
- Inability to get access to management: 47%
- Competitive time pressures: 47%
- Lack of warranties and indemnities: 43%
- Environmental issues: 36%
- Inability to restructure effectively: 29%
- Underfunded pension scheme: 19%
- Price issues: 14%

DUE DILIGENCE

- A term used for a number of concepts involving either an investigation of a business or person, or an action with a certain standard of care.
- It can be a legal obligation, but the term will more commonly apply to voluntary investigations.
- It is more common than you think since it is required for some many activities
  - associating with other companies
  - hiring employees
  - taking on new clients
REPUTATIONAL GAPS- WHEN REPUTATION EXCEEDS REALITY
WHEN REPUTATION EXCEED REALITY

Insufficient Due Diligence - Effect of Lack of Information
The due diligence process will pick it up
His references check out
My people checked him out
I have already gotten to know him
I’ve met him -- he’s fine
WHAT A CANDIDATE WILL NEVER TELL YOU

Dear CFO,

I have been stealing from our company for years and now I can’t sleep nights. Please accept this $5,000.00 check. If I still can’t sleep, I will send the rest!

Thank you.

COMPANY X
PRIVATE/ PUBLIC PARTNERSHIP: A SOURED CORPORATE MARRIAGE
RENAVE – RICARDO CAVALLO & TALSUD
REPUTATIONAL GAPS – ERODED REPUTATION
ERODED REPUTATION

Effect of Rumors or Bad Press

Eroded Reputation

Reality

“Gap”

Negative Effect on Price
“Sudan wants U.N. to probe U.S. bombing of drug factory”

“Sudan says that the U.S. bombing of the factory was based on “faulty intelligence”
SEVEN WARNING SIGNS
SIETE SEÑALES DE ADVERTENCIA

• Lack of Experience in industry or projects
• Experience in unregulated industries
• Owners or management
  o provide scarce details or lack of precision
  o Insufficient financial information
• Complicated ownership structures
• Past criminal and or civil litigation
WORKSHOP
WORKSHOP AGENDA

- Introduction to Risk Management
- Reputational Risk & Exercise
- Risk and Public Financial Management Planning
- Problem of Risk Avoidance
- Risk Matrix & Exercise
- Governance, Risk & Compliance Software
- Planning Tools Integration
- IT Risk Management
- Risk Management Maturity & Exercise
- Using This with Your Government
BUDGET CYCLE

- Budget Preparation
- Budget Execution
LINKED TO BUDGET PLANNING

Macroeconomic Framework

Government Priorities

Risk Management

Budget Plan
FEEDBACK LOOP

1. Macroeconomic Framework
   - Financial results

2. Government Priorities
   - Outcomes

3. Risk Management
   - Risks realized, risks avoided, risk impacts

Budget Plan

Actuals

Monitoring & Evaluation
BUDGET CYCLE RISKS

- Forecasting
- Fiscal Space

Budget Preparation

- Arrears
- Liquidity
- Corruption
- Inefficiency
- Outcomes

Budget Execution
CONSIDER PUBLIC INVESTMENT PROJECTS
## GOVERNMENT CONCERNS

<table>
<thead>
<tr>
<th></th>
<th>Policy</th>
<th>Operational</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Political</strong></td>
<td>Will project be completed within the current Government mandate?</td>
<td>Will project be on time?</td>
</tr>
<tr>
<td><strong>Contractual</strong></td>
<td>Will vendors complain about unfair practices?</td>
<td>Will the right solution / best value be acquired?</td>
</tr>
<tr>
<td><strong>Programmatic</strong></td>
<td>Did the expected outcomes occur?</td>
<td>Will project be on budget?</td>
</tr>
</tbody>
</table>
## Interpretation of Failure

<table>
<thead>
<tr>
<th>Category</th>
<th>Policy</th>
<th>Operational</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Political</strong></td>
<td>Proves policy ineffectiveness</td>
<td>Civil servants did not have competence to execute policy</td>
</tr>
<tr>
<td><strong>Contractual</strong></td>
<td>Proves policy was too expensive to have benefits</td>
<td>Civil servants unable to choose most effective solution</td>
</tr>
<tr>
<td><strong>Programmatic</strong></td>
<td>Proves policy was too difficult to have benefits</td>
<td>Civil servants were not able to manage the project on time &amp; on budget</td>
</tr>
</tbody>
</table>
## EFFECTIVE RISK MANAGEMENT BENEFITS

<table>
<thead>
<tr>
<th>Innovative</th>
<th>Policy</th>
<th>Operational</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Government is world leader in innovation.</td>
<td>Low cost with high benefits thanks to leveraging innovative solutions.</td>
</tr>
</tbody>
</table>
WHEN DISASTER STRIKES
MOTIVATION FOR PFM REFORM
WORKSHOP AGENDA

- Introduction to Risk Management
- Reputational Risk & Exercise
- Risk and Public Financial Management Planning
- Problem of Risk Avoidance
- Risk Matrix & Exercise
- Governance, Risk & Compliance Software
- Planning Tools Integration
- IT Risk Management
- Risk Management Maturity & Exercise
- Using This with Your Government
HEURISTICS AND BIAS
COMMON BIASES

- Excessive optimism
- Overconfidence
- Confirmation Bias
- Groupthink
- Control Bias
- Loss Aversion
- Sunk-cost Fallacy
- Status Quo Bias
EVALUATION
RISK CALCULATION
LIKELIHOOD
CAN’T ELIMINATE BIAS
WORKSHOP AGENDA

- Introduction to Risk Management
- Reputational Risk & Exercise
- Risk and Public Financial Management Planning
- Problem of Risk Avoidance
- Risk Matrix & Exercise
- Governance, Risk & Compliance Software
- Planning Tools Integration
- IT Risk Management
- Risk Management Maturity & Exercise
- Using This with Your Government
RISK CALCULATION

RISK = NEGATIVE LIKELIHOOD X NEGATIVE IMPACT
## TRADITIONAL RISK MATRIX

<table>
<thead>
<tr>
<th>Negative Likelihood</th>
<th>Low</th>
<th>Medium Low</th>
<th>Medium</th>
<th>High</th>
<th>Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mitigate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avoid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Negative Impact
- Very High
- High
- Medium
- Medium Low
- Low

*Colors indicate risk levels: Green (Low), Yellow (Medium), Orange (High), Red (Very High).*
INNOVATION CALCULATION

INNOVATION =

(LIKLIHOOD OF POSITIVE RESULT X POSITIVE IMPACT) - (LIKLIHOOD OF NEGATIVE RESULT X NEGATIVE IMPACT)
## BENEFIT MATRIX

<table>
<thead>
<tr>
<th>Positive Likelihood</th>
<th>Low</th>
<th>Medium Low</th>
<th>Medium</th>
<th>High</th>
<th>Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Very High</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPROACH: INNOVATION APPETITE
## APPROACH

### Negative Impact vs. Negative Likelihood

<table>
<thead>
<tr>
<th>Negative Impact</th>
<th>Low</th>
<th>Medium Low</th>
<th>Medium</th>
<th>High</th>
<th>Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>Orange</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
<td>Orange</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
<td>Orange</td>
<td></td>
</tr>
<tr>
<td>Medium Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Orange</td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Based on risk appetite, should not engage in projects of high risk.
## APPROACH

<table>
<thead>
<tr>
<th>Positive Impact</th>
<th>Very High</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td></td>
<td>Based on innovation appetite, should not engage in projects of low return &amp; probability</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Medium Low</td>
</tr>
</tbody>
</table>

### Positive Likelihood

- Low
- Medium Low
- Medium
- High
- Very High
NEW MATRIX

High positive impact, High positive likelihood
Low negative likelihood

High negative impact
High negative likelihood

Low positive impact, Low positive likelihood

Accept  Monitor  Mitigate  Avoid
Problem Description

Overview: Decentralized organizations may code transactions from a budget area where they have no budget left to areas where they have budget.

Narrative: Although decentralized entity is not overspending, the government needs realistic budget information for realistic planning. Decentralized budget entities have sufficient discretion of to support minor budget virements, all other transfers should be approved by the Ministry of Finance.

Solution Description

* Mitigation: Decentralized officers training course.

* Monitor: MoF will examine monthly budget transfer reports & audit those that have less than 5% virements.

* Reasoning: Unrealistic for decentralized entities to operate consistently without virements. Training course will help officers understand that virements will be generally accepted, that they have sufficient authority & need for more accurate budgets for the following year.
WORKSHOP
WORKSHOP AGENDA

• Introduction to Risk Management
• Reputational Risk & Exercise
• Risk and Public Financial Management Planning
• Problem of Risk Avoidance
• Risk Matrix & Exercise
• Governance, Risk & Compliance Software
• Planning Tools Integration
• IT Risk Management
• Risk Management Maturity & Exercise
• Using This with Your Government
GRC – ANOTHER TECH INDUSTRY “TLA”*
ERM – ANOTHER TECH INDUSTRY “TLA”*

* Three Letter Acronym

Governance

Enterprise Risk Management

Compliance

Risk
GOVERNANCE

• Structure of how organization achieves goals
RISK

- Anticipating and managing risks
COMPLIANCE

• With organizational policies & procedures
SYNCHRONIZED
THEREFORE – BUDGET INTEGRATION
WORKSHOP AGENDA

- Introduction to Risk Management
- Reputational Risk & Exercise
- Risk and Public Financial Management Planning
- Problem of Risk Avoidance
- Risk Matrix & Exercise
- Governance, Risk & Compliance Software
- Planning Tools Integration
- IT Risk Management
- Risk Management Maturity & Exercise
- Using This with Your Government
DEALING WITH UNCERTAINTY
PESTEL

- political
- economical
- societal
- technological
- environmental
- legal
PREDICTABILITY
ODDS
WORKSHOP AGENDA

• Introduction to Risk Management
• Reputational Risk & Exercise
• Risk and Public Financial Management Planning
• Problem of Risk Avoidance
• Risk Matrix & Exercise
• Governance, Risk & Compliance Software
• Planning Tools Integration
• IT Risk Management
• Risk Management Maturity & Exercise
• Using This with Your Government
REPUTATION & IT - THE HUMAN FACTOR

David A. Robillard, President – MultiLatin
February 2014
TRENDING TOPICS

https://www.privacyassociation.org/privacy_perspectives/post/2013_the_year_of_privacy
The (not so) secret life of the NSA.
EXTRACTING VALUE FROM INFORMATION CHAOS
WHY GOOD GOVERNANCE MAKES GOOD SENSE

BYOD (BRING YOUR OWN DEVICE)

 SECURITY BREACHES

 CYBERCRIME COSTS
US $1 TRILLION
PER YEAR

 MALWARE SAMPLES
75M
IN 2012

 DATA PROLIFERATION

 SOCIAL MEDIA RISK

 PRIVACY REGULATIONS

 DOWNTIME

 2 OUT OF 3 COMPANIES
ARE AT RISK
FROM SOCIAL MEDIA INCIDENTS

 8 OUT OF 10
EMPLOYEES
AGE 16-35
USE A PERSONAL
DEVICE FOR WORK

 24B
CONNECTED DEVICES
BY 2020

 THE AVERAGE CORPORATE
WORKER SENDS & RECEIVES
112 EMAILS
PER DAY

 AVERAGE COST
$5,000
A MINUTE
FOR DOWNTIME

 $380B
AVG. COST
OF DOWNTIME
IN 2011

 9.6 MILLION
TERABYTES
OF INFORMATION
PROCESSED BY THE WORLD'S
COMPUTERS
IN 2011

http://www.isaca.org/COBIT/Pages/default.aspx
DATA BREACHES - PEOPLE & PARTNERS

Data breaches in business worldwide

Compromised records by type of threat worldwide, 2004-11

Current and projected percentages of mobile device users with single and multiple devices worldwide

Source: Verizon

### Online Banking

Transactions get riskier as cybercriminals use cheaper, more sophisticated tools.

**Prices (in US$):**

- **LATIN AMERICA:** $190.00 for PiceBOT, crimeware kit for stealing banking data
- **RUSSIA:** copies of credit cards, passports, work permits

**Facts:**

- 112,981 Online Banking Malware Victims in Q1 2013
- **US$ 225,334** Amount made by China's Topfox Case Gang on online banking theft

### Email

Even with advanced spam filtering, you're still prone to spam.

**Prices (in US$):**

- **Email spamming and flooding tool:** $30
- **Email flooding service per 1,000 emails:** $2
- **Spamming service per 1,000,000 emails:** $10

### Online Gaming

The popularity of in-game purchases have made gamers prime cybercriminal targets.

**Facts:**

- **5.3 BILLION** Game credentials stolen by China's Blandroid Gang in 2009
- **US$ 225 M** Online game assets stolen by cybercrime groups in 2011

### Bad Patching Practices

With how exploit kits are being traded, users who forgot patching put their data in danger.

**Prices (in US$):**

- **Rental of STYX Exploit Pack per month:** $3,000
- **25 rental of exploit kit bundles per day:** $25
- **Minimum price for individual exploit kits:** $2,500

### General Browsing

Cybercriminal threats are now less detectable by traditional security software.

**Prices (in US$):**

- **Weekly/monthly anti-malware evasion service:** $0.15-25
- **CHINA:** Compromised webhost $0.01-1.0
- **RUSSIA:** 1,000 artificial traffic per SEO $5
- **RUSSIA:** Automation tools for blackhat SEO $295
- **100-500:** Pay-per-install services

### Mobile Browsing

Mobile device users can expect more attacks to come via their gadgets.

**Prices (in US$):**

- **3 to 150:** SMS spamming services per 100-10,000 messages
- **100:** RUSSIA: SMS delivery tool using fake numbers

### Social Networking & Messaging

New cybercriminal tools make hacking your social network accounts easier.

**Prices (in US$):**

- **5:** Fullz (full personal info sheets)
- **97:** RUSSIA: Hacking tools for Gmail and other email accounts
- **130:** RUSSIA: Facebook and Twitter hacking service
- **500:** Corporate email hacking service (per mailbox)

---

https://paladinsecurity.com/blog/safety-security-tips/cybercriminal-underground-infographic-tips-protect-your-privacy
COSTS OF BREACHES

Data Breach Costs Soar Even Higher

Businesses Paid an Average of $7.2 Million per Data Breach in 2010
That’s an Average of $214 per record

Rapid response to data breaches is costing companies 54% more per record

Negligence is the most common threat, causing 41% of breaches

Malicious attacks are most expensive and more frequent: 31% of breaches

61% deploy Encryption after a data breach. Top post-breach remedy is training and awareness programs at 63%

Only 27% of breaches caused by system glitches

TYPES OF ATTACKS

Motivations Behind Attacks (2013)
- Cyber Crime: 47%
- Hacktivism: 44%
- Cyber Espionage: 5%
- Cyber Warfare: 4%

Top Targets (2013)
- Government: 47%
- Industry: 22%
- Finance: 14%
- Organisation: 6%
- 3%
GOVERNANCE EXPECTATIONS

Security

Data Protection/Privacy

Controls
FRIENDS OR FOES?

Security and Privacy: Two Faces of the Same Coin

Security: Outward Facing

Privacy: Inward Facing

https://www.privacyassociation.org/privacy_perspectives/post/2013_the_year_of_privacy
Security Legislation

Interactive Data Protection Heat Map

Source: US Department of Commerce and country specific legislation

[Map showing data protection regulations around the world with different colors indicating levels of restrictions and cautions for government surveillance.]

Source: Forrester Research, Inc.
TRADITIONAL SECURITY MODEL

Human Factors

Procedures/Process

Technology
SECURITY COMPLIANCE MODEL

Human Factors

All fits within compliance standards for organizational conduct and screening

Procedures / Process

Technology
MOTIVES FOR MISUSE OF POSITION

- Ideology or higher calling
- Financial (greed or need)
- Revenge
- Challenge or curiosity
- Power
For me, in terms of personal satisfaction, the mission’s already accomplished,” he said.

“I already won. As soon as the journalists were able to work, everything that I had been trying to do was validated.

Because, remember, I didn’t want to change society. I wanted to give society a chance to determine if it should change itself.
HEROES OR DEVILS?
Depressed with the situation we were mired in [in Iraq]," and dismayed by counterterrorism operations in which the U.S. seemed "obsessed with capturing and killing people,"

Manning said he’d sought to "make the world a better place". 
MOTIVES FOR MISUSE OF POSITION

- Financial (greed or need)
- Entitlement or envy
- Challenge or curiosity
- Power
- Ideology or higher calling
Cybercrimes

What It Is:
Cybercriminals treat cybercrime as a legitimate business—selling information, tools, and resources

Fact:
Russia: Nearly every kind of exploit and hack can be bought for a price

What It Means:
Treated as a business, cybercriminals not only profit from your data, they also gain by helping out other cybercriminals do the same

What It Is:
Cybercriminals work in groups, with each member assigned an important role in the process

Fact:
2008: the Topfox gang coordinated via the Internet and laundered stolen property before converting it to cash

What It Means:
Due to their organized structure, it's harder to track cybercriminals or recover your stolen resources

Organized Crime Business Model

https://paladinsecurity.com/blog/safety-security-tips/cybercriminal-underground-infographic-tips-protect-your-privacy
What It Is: Cybercriminals outsource, hiring computer owners to join their cybercriminal botnet
Fact: 2009: Swordsman DDoS attacks used a botnet against a game server, managing to extort US$ 3,107.87 from a game company

What It Means: With more affordable botnets, account theft is now more common

What It Is: Cybercriminals train others who are interested in learning the craft
Fact: China: Underground ads “seeking a master” outnumber ads “seeking an apprentice” by 54%, ensuring new blood

What It Means: Through passed-on techniques and practices, new cybercriminals come up with more sophisticated attacks

Africa will soon be the next cybercriminal haven due to developing infrastructure and lack of cybercrime laws

Cybercrime in Latin America rose 40% from 2011 to 2012

Cybercriminals now sell more for less
2012 price: US$3 = credit card number only
2013 price: US$5 = fullz info

https://paladinsecurity.com/blog/safety-security-tips/cybercriminal-underground-infographic-tips-protect-your-privacy
According to ACFE in 81% of cases fraudsters display one or more behavioral red flags that are often associated with fraudulent conduct.

- 36% living beyond means
- 27% financial difficulties
- 19% had unusually close association with vendors or customers and
- 18% had excessive control issues
MOTIVES FOR MISUSE OF POSITION

- Ideology or higher calling
- Financial (greed or need)
- Revenge
- Challenge or curiosity
- Power
EXAMPLE – DATA PRIVACY

Theft of Electoral Roll in México - IFE

http://noticieros.televsia.com/mexico/1311/ife-ifai-presentan-denuncia-pgr-filtracion-datos/
EXAMPLE – DATA PRIVACY

Theft of Electoral Roll in México - IFE

Multiple Uses including Targetting HNWI Victims for Extortion and Kidnapping

http://noticieros.televisa.com/mexico/1311/ife-ifai-presentan-denuncia-pgr-filtracion-datos/
MOTIVES FOR MISUSE OF POSITION

- Ideology or higher calling
- Financial (greed or need)
- Revenge
- Challenge or curiosity
- Power
CHALLENGE OR CURIOSITY

Is it a game, or is it real?
MOTIVES FOR MISUSE OF POSITION

- Ideology or higher calling
- Financial (greed or need)
- Revenge
- Challenge or curiosity
- Power
MOTIVES FOR MISUSE OF POSITION

- Financial (greed or need)
- Ideology or higher calling
- Revenge (entitlement)
- Challenge or curiosity
- Power

..........and of course........
there’s always ..........
...........mistakes or errors
BEST PRACTICES

- Physical Security.
- Data Classification and Retention.
- Password Requirements and Guidelines.
- Wireless Networking.

http://www.corporatecomplianceinsights.com/information-security-best-practices/
Employee Awareness Training
Incident Response.
CLOSING REMARKS

- The Internet of Things
  - Opportunity and risk

- Organizations consist of people
  - Employees and third party partners
  - Systems can’t distinguish between an authentic and a false user
  - Know the people who have both physical and systems access

- Within your respective Governments
  - the data is more valuable than the money
  - ability to operate 24/7 may be at risk
CLOSING REMARKS

- Your constituents and stakeholders depend upon your ability to protect their data from theft, misuse or destruction.

- Risks to your Governments may include financial costs, damage to reputation and confidence.

- The costs to your constituents may go beyond and include personal and financial losses.

http://www.corporatecomplianceinsights.com/information-security-best-practices/
WORKSHOP AGENDA

• Introduction to Risk Management
• Reputational Risk & Exercise
• Risk and Public Financial Management Planning
• Problem of Risk Avoidance
• Risk Matrix & Exercise
• Governance, Risk & Compliance Software
• Planning Tools Integration
• IT Risk Management
• Risk Management Maturity & Exercise
• Using This with Your Government
FOR EVERYONE
CONSIDER MATURITY

Level 0: Absent
Level 1: Initial
Level 2: Repeatable
Level 3: Defined
Level 4: Managed
Level 5: Optimized
MATURITY APPROACH

0: Absent
1: Initial
2: Repeatable
3: Defined
4: Managed
5: Optimized
MATURITY APPROACH

- Focus on where capacity is high
WORKSHOP
WORKSHOP AGENDA

- Introduction to Risk Management
- Reputational Risk & Exercise
- Risk and Public Financial Management Planning
- Problem of Risk Avoidance
- Risk Matrix & Exercise
- Governance, Risk & Compliance Software
- Planning Tools Integration
- IT Risk Management
- Risk Management Maturity & Exercise
- Using This with Your Government
SUMMARY

• Risky approach = risk avoidance
• Often unaware of status quo risks
• Risk can be managed effectively
• Risk tools can be leveraged
• Government risk management is special & critical for government performance
• Many government underestimate IT risks