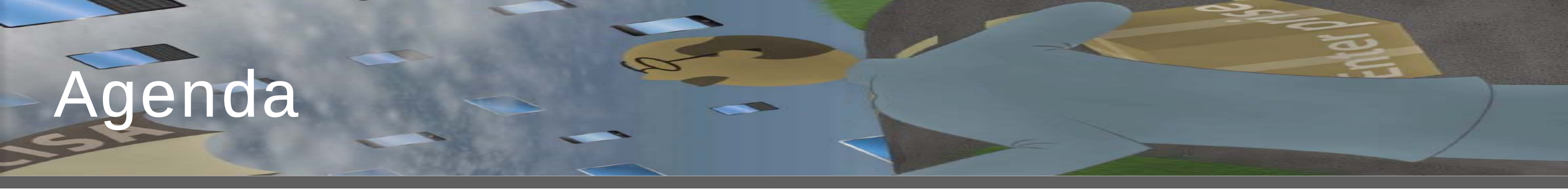
Quantifying Risks & Controls

Methods that Work - Methods that Don’t

Aidan Collins
CEO, ControlMetric, Inc.

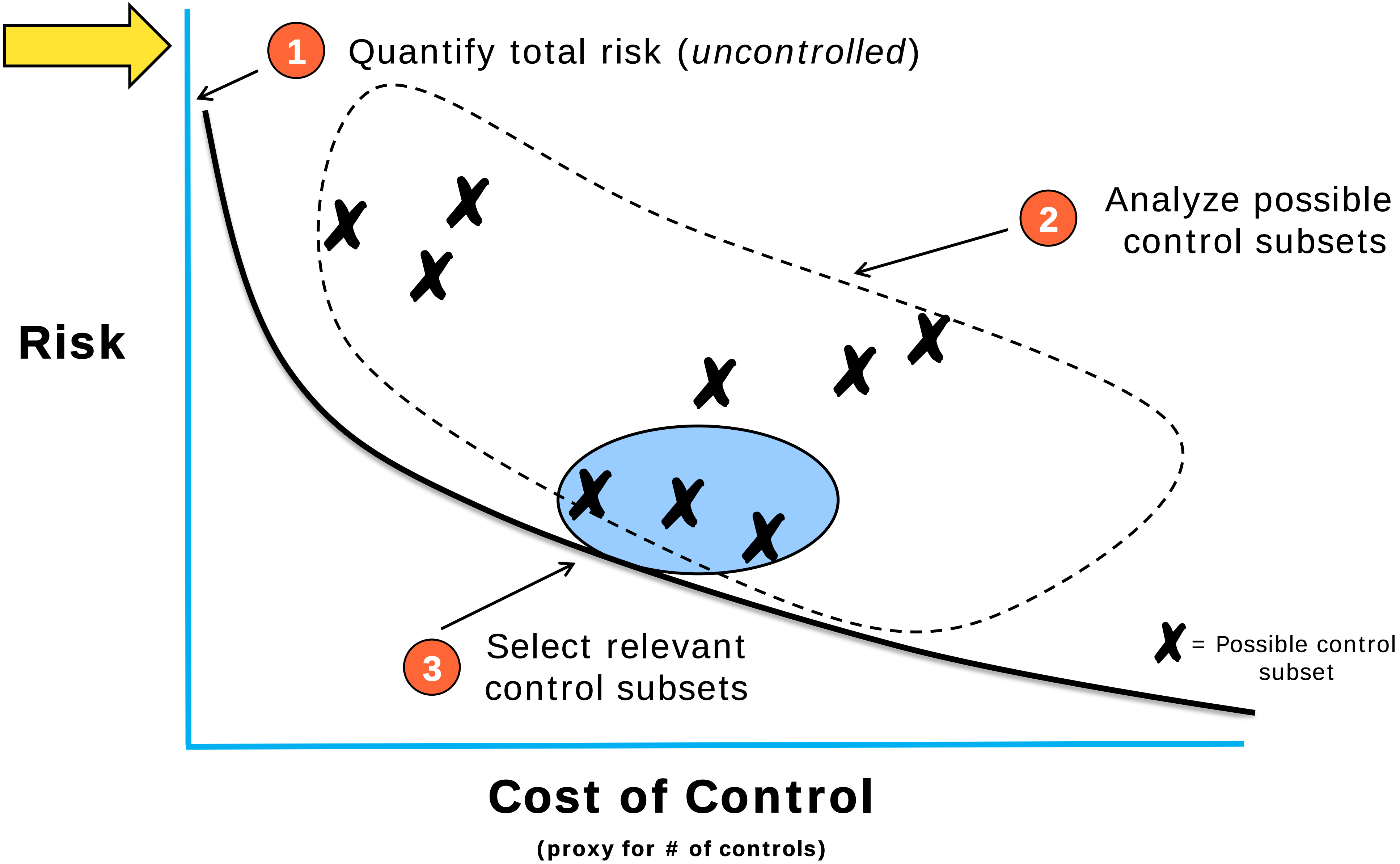
Governance, Risk & Compliance - G23



Agenda

- Introduction
- Estimating the size of risk
- Measuring the mitigation effect of controls
- Summary/wrap up

Overall problem is to find “best” set of controls to mitigate a risk

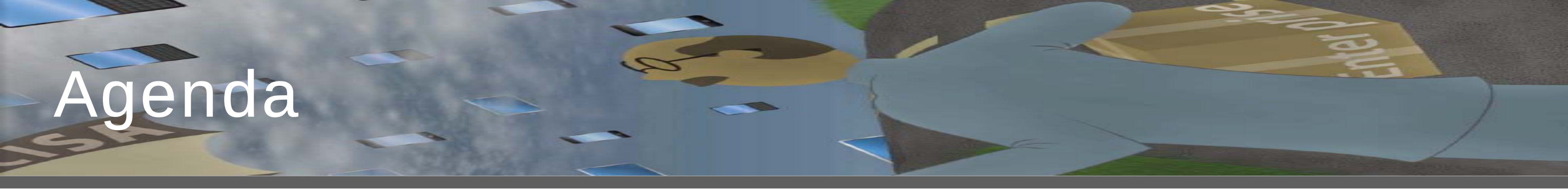


1 Quantify total risk (*uncontrolled*)

2 Analyze possible control subsets

3 Select relevant control subsets

✗ = Possible control subset

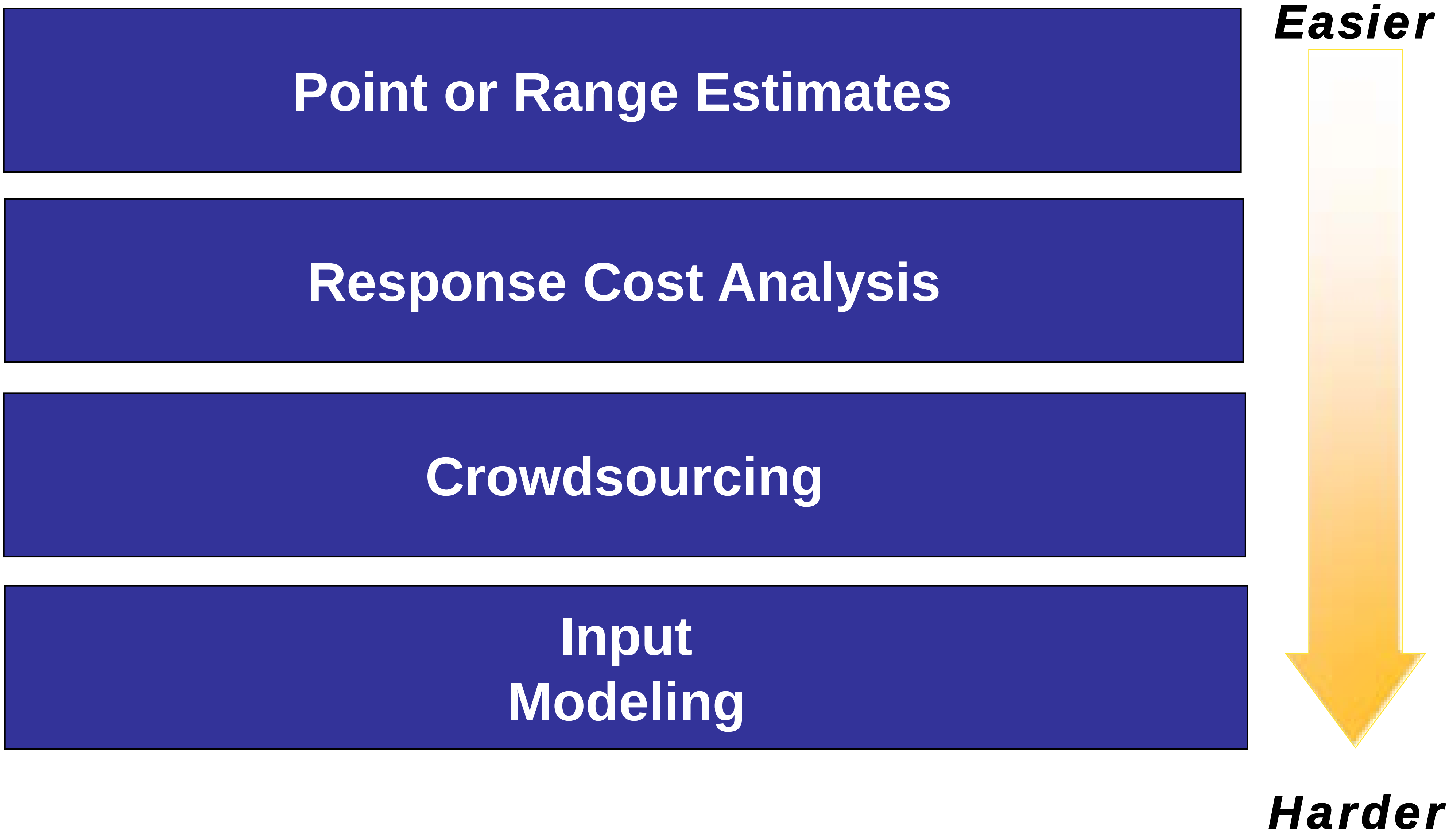


Agenda

- Introduction
- Estimating the size of risk
- Measuring the mitigation effect of controls
- Summary/wrap up

This information is confidential and was prepared by ControlMetric solely for the use of our client; it is not to be relied on by any 3rd party without ControlMetric's prior written consent.

Several different approaches can be used to quantify risk



Point or Range Estimates

Response Cost Analysis

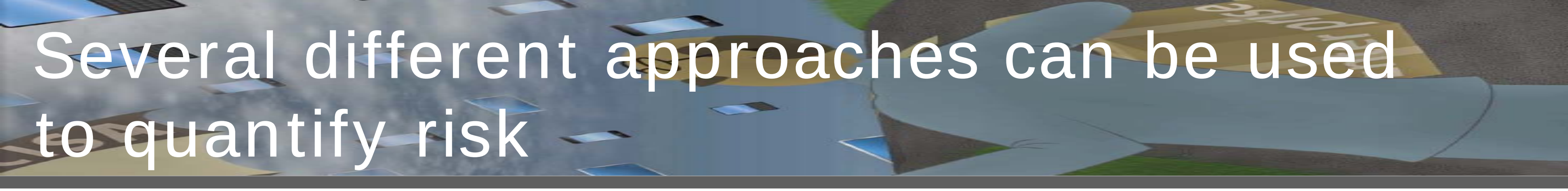
Crowdsourcing

Input Modeling

Several different approaches can be used to quantify risk

Point or Range Estimates

- Can be generated either **externally** (e.g. industry benchmark) or **internally** (e.g. planning assumption)
- Often backed by **historical experience** or **external analysis**
- For example, external benchmark for risk of “shadow payroll” fraud is **0.1% of total payroll**

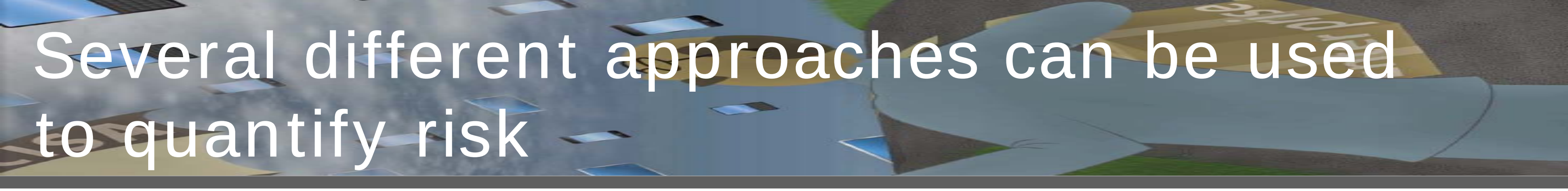


Several different approaches can be used to quantify risk

Response Cost Analysis

- **Focus on responses** to risk occurrence as an estimate of the risk impact
- Responses are categorized and **cost estimates are generated** for each response
- Can either be a **point or range** estimate

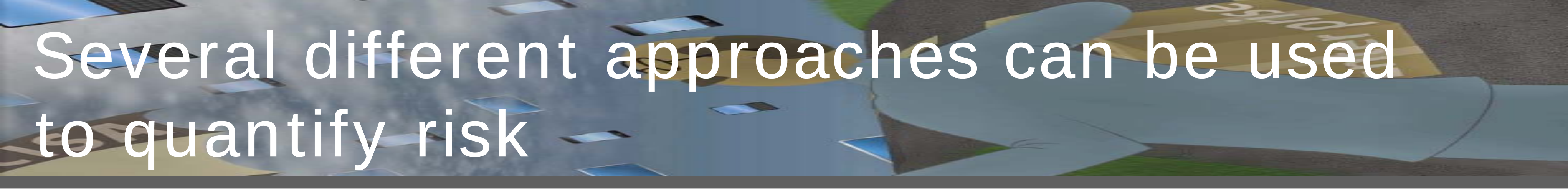
This information is confidential and was prepared by ControlMetric solely for the use of our client; it is not to be relied on by any 3rd party without ControlMetric’s prior written consent.



Several different approaches can be used to quantify risk

Crowdsourcing

- Uses the **power of many opinions** to generate a more reliable estimate of risk
- Can be generated either **internally to the organization** or, in some cases, can be **extended to business partners**
- Can be extended to include **prediction markets**

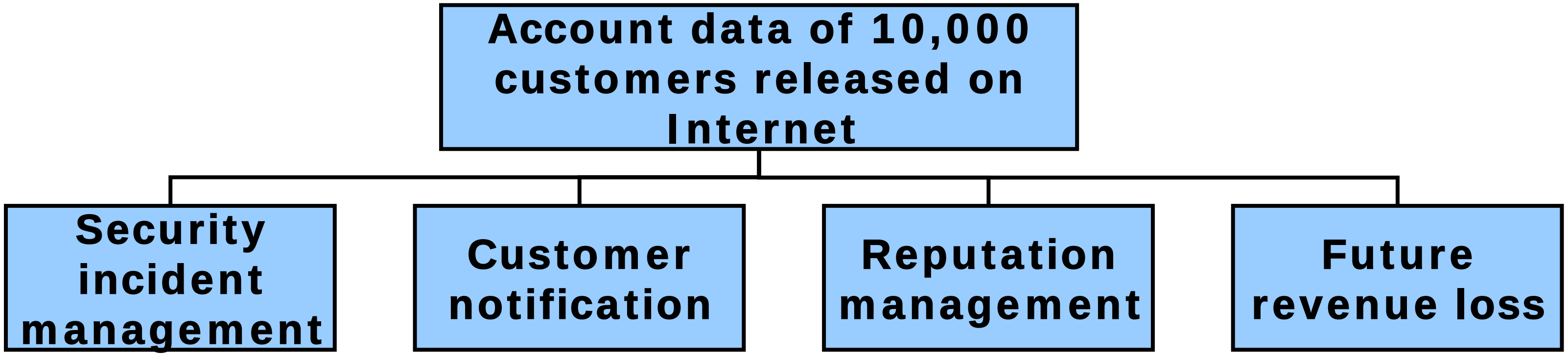


Several different approaches can be used to quantify risk

Input Modeling

- **Decompose risk** down to input variables impacting the likely outcome of risk
- Decide on **statistical distribution** for each input variable
- **Model range** of input variables to generate distribution of likely risk values, e.g. **Monte-Carlo**

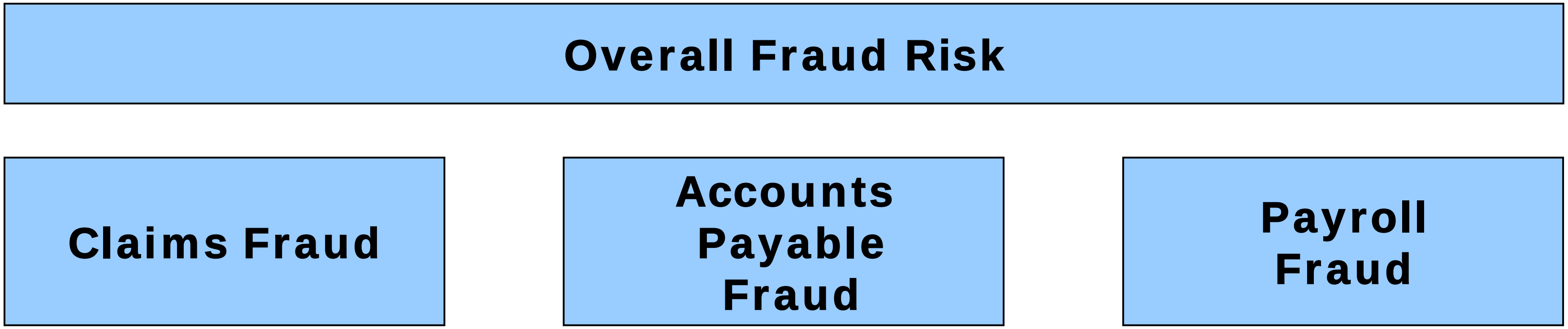
For example, analyzing response costs can be useful in sizing data security risks…



Risk	**Account data of 10,000 customers released on Internet**			
Responses	**Security incident management**	**Customer notification**	**Reputation management**	**Future revenue loss**
Actions	- Conduct emergency security audit - Apply security patches	- Notify and follow-up with impacted customers - Provide and activate credit monitoring	- Pay fines for non-compliance - Increased communication to customers and regulators	- Impacted customers reduce spending by 80% for six months - Web traffic reduced by 5% for one week
Estimated Total Cost	**$500K**	**$600K**	**$1.2M**	**$3.4M**

Total cost of response is approximately $5.7M – this becomes the estimate of risk

…while decomposing risk to its components can work for business risks…



- **Historical experience** of claims fraud is in the range of 3-4% of incurred losses
- **Industry data** suggests 10% of incurred losses represent claims fraud

- **Industry data** suggests 5% total revenue is lost to all fraud
- **Average loss per incident** related to disbursements in the range $20-125k

- **No historical experience** of payroll related fraud
- **Industry averages** are in the range of 1% of total payroll expense

Claims fraud risk dominates; overall fraud risk estimated at $12M

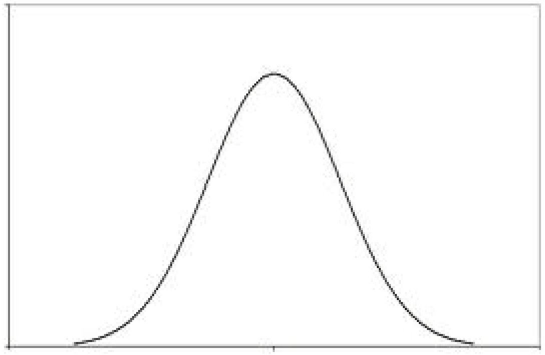
This information is confidential and was prepared by ControlMetric solely for the use of our client; it is not to be relied on by any 3rd party without ControlMetric’s prior written consent.

…and Monte-Carlo modeling of project inputs can help assess ROI risk

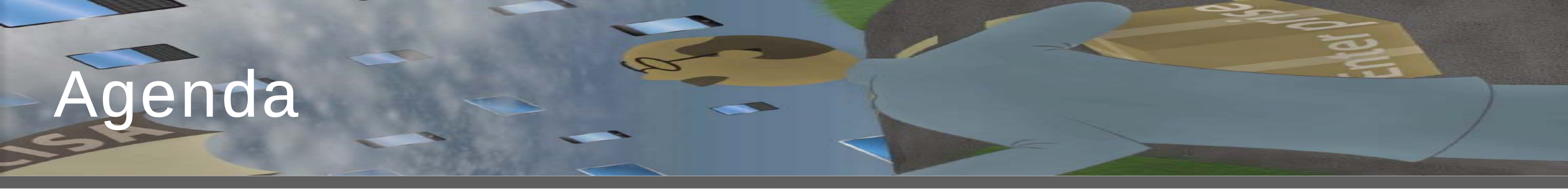
- Time to complete system – 12 to 18 months
- Cost of new system - $4M to $8M
- Predicted agent adoption – 40% to 70%
- Additional revenue per agent - $500K to $1.5M
- Margins on additional revenue – 20% to 25%
- New system operating costs - $140K to $300K
- Internal productivity savings with new system - $400K to $700K

Input factors influencing project ROI

Model these inputs to generate estimate of project ROI

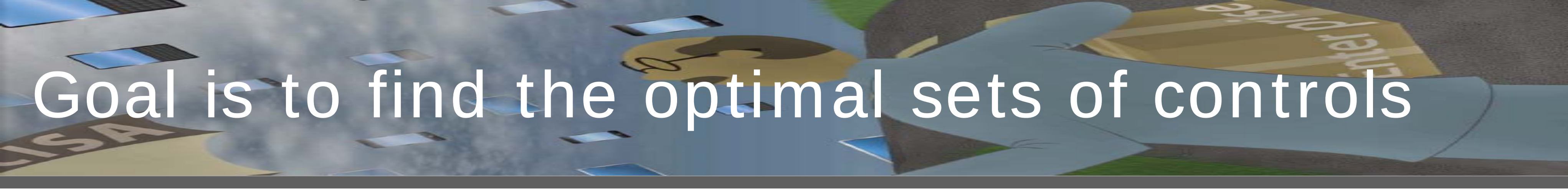


90% Confidence Interval of expected ROI is -5% to +18%. This provides an estimate of the ROI risk.



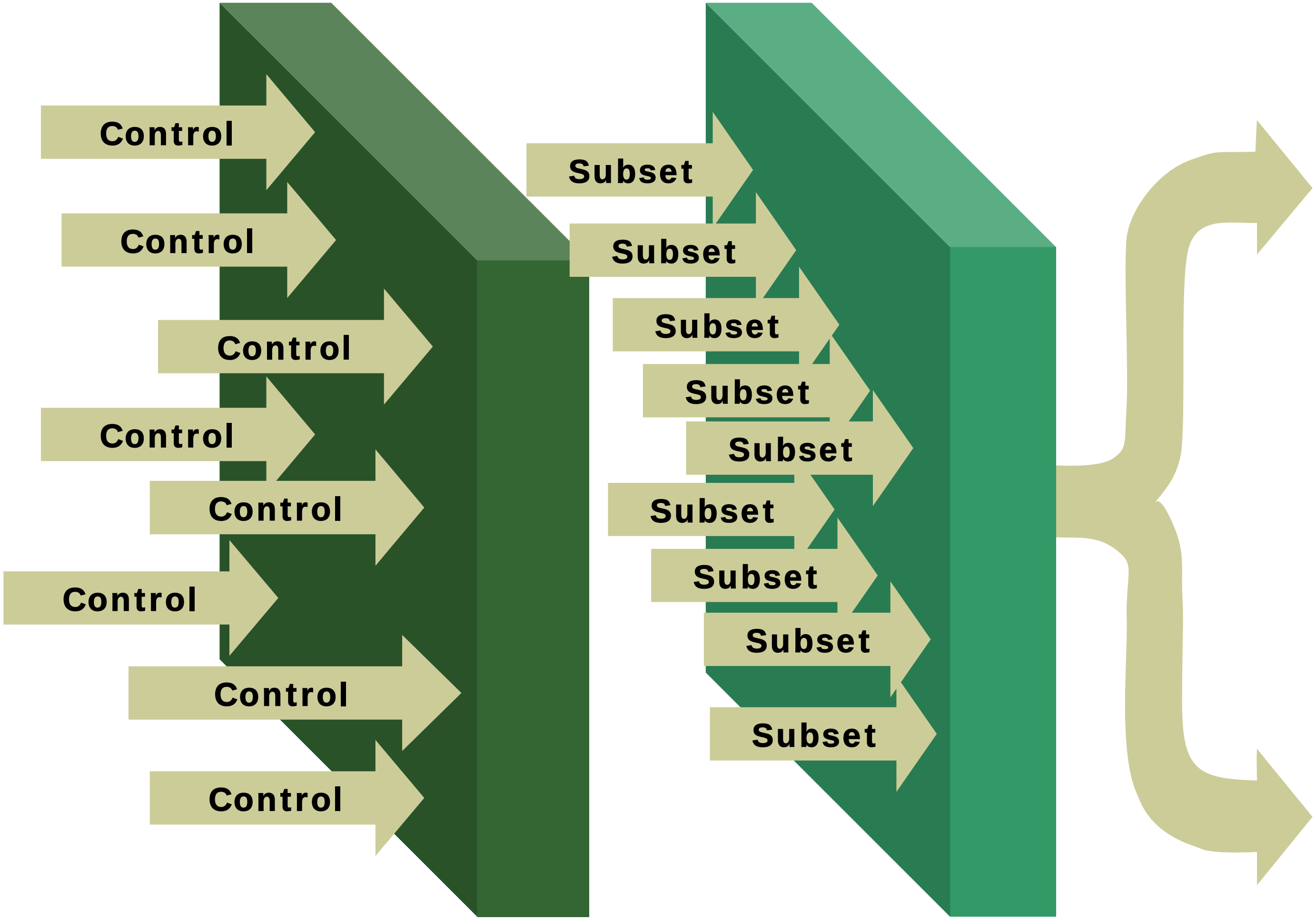
Agenda

- Introduction
- Estimating the size of risk
- Measuring the mitigation effect of controls
- Summary/wrap up



Goal is to find the optimal sets of controls

Universe of Controls ***All possible subsets*** ***Ranking of viable subsets***



- **All possible subsets of controls**
- **Ordered on process risk mitigation**
- **Includes "mandated" controls (e.g. regulatory requirement)**
- **Addition of cost information enables "efficient frontier"**

Includes all sources of control

Rank-Order Model

This information is confidential and was prepared by ControlMetric solely for the use of our client; it is not to be relied on by any 3rd party without ControlMetric's prior written consent.

Generate effectiveness and cost data for each control

Coverage

- For a specific risk, how **much of that risk is mitigated** assuming the control is operational at all time

Operation

- This is an estimate of how **often this control works** over time

Flexibility

- This measures how well this individual control can deal with **minor anomalies** related to the risk being mitigated

Combine to generate an overall control effectiveness score for each control

Cost

- What are the **estimated costs** associated with this control?

Generate the data to be used to as input to the Rank-Order Model

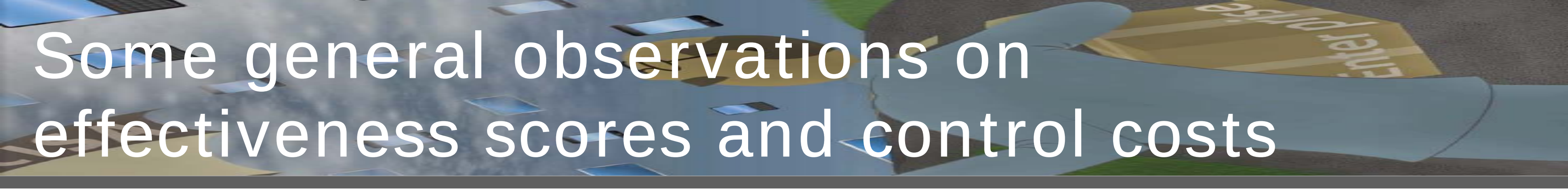
This information is confidential and was prepared by ControlMetric solely for the use of our client; it is not to be relied on by any 3rd party without ControlMetric's prior written consent.

Controls are scored based always on the *particular* risk being mitigated

“Users have more access privileges in excess of those needed for their roles”

Control scores (Coverage, Operational, Flexibility)

Ref.	***Control***	***Cov.***	***Oper.***	***Flex.***	***Cost***
1	Information security standards and guidelines exist. These standards and guidelines serve as the basis for security administration, management, and monitoring. This policy also defines the responsibilities of our Information Security Officer, users and management.	0.4	0.5	0.85	$300K
2	An Information Security awareness program exists and is updated on an annual basis.	0.4	0.5	0.85	$500K
3	Generic user accounts (e.g., Temp01) are not used to access and perform transactions within business applications.	0.65	0.85	0.9	$50K
4	Each business user is assigned a unique account using a standard naming convention to ensure accountability for each user.	0.85	0.5	0.9	$25K
5	All requests for new user access to App/DB/OS/Network are submitted in writing by an individual authorized to approve access.	0.8	0.4	0.8	$25K
6	Employee terminations are communicated by HR or management, in a timely manner. Accounts are disabled/removed in a timely manner.	0.7	0.3	0.9	$35K
7	All user access additions and modifications made in the App/DB/OS/Network are documented and maintained.	0.5	0.3	0.8	$50K
8	Reports of current App/DB/OS/Network access privileges are periodically generated and distributed to process/data owners for review. Process/data owners validate propriety of access rights. Access privileges are modified as appropriate.	0.8	0.5	0.7	$75K

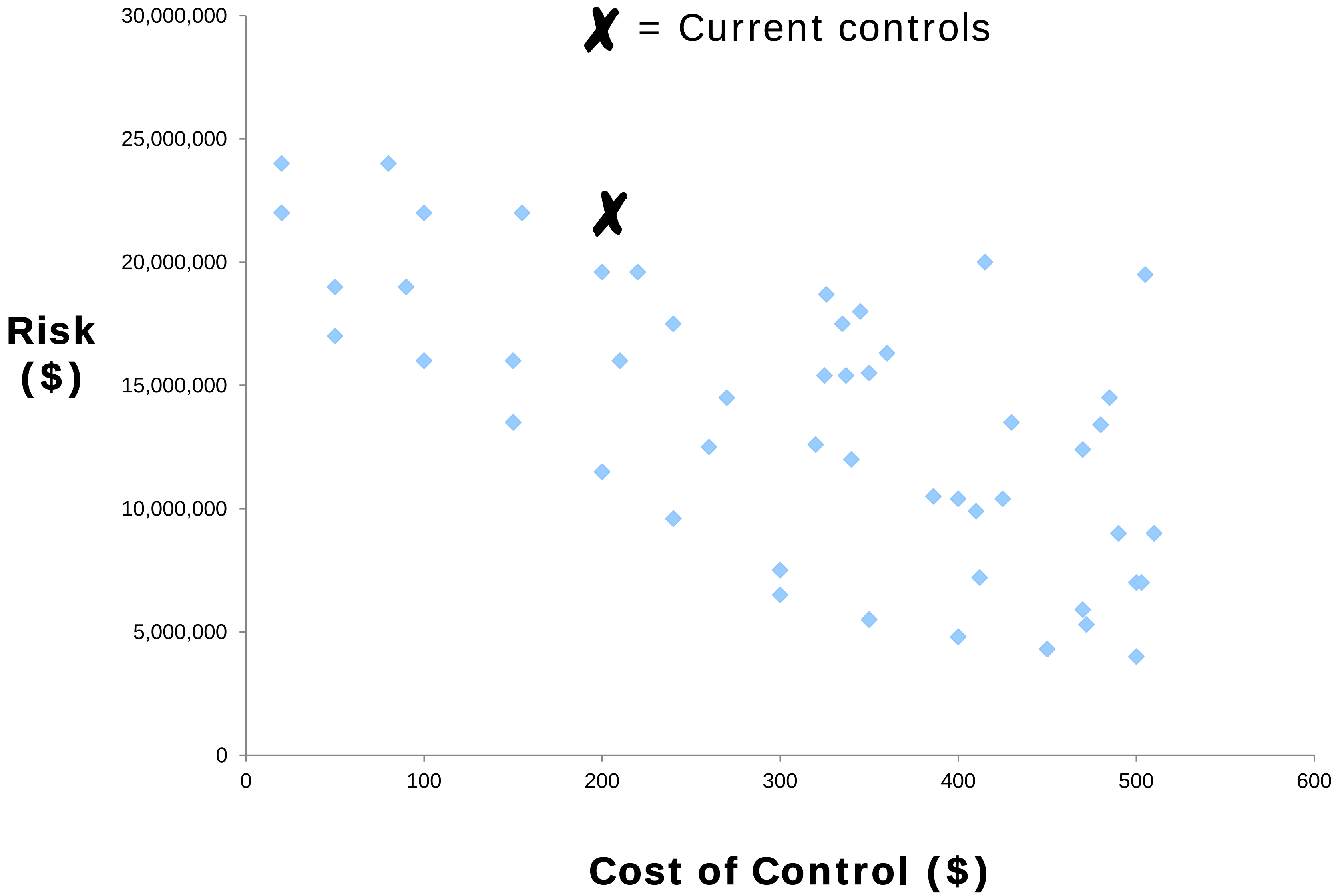


Some general observations on effectiveness scores and control costs

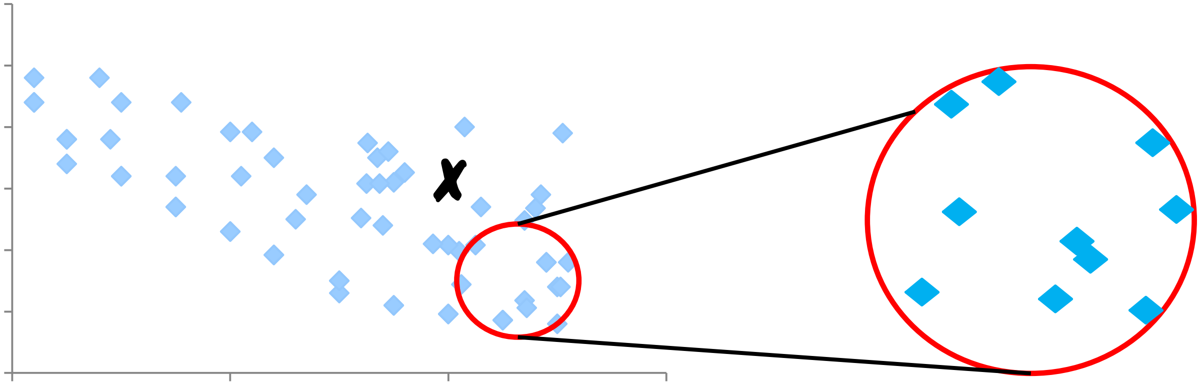
Observations	Implications
• Scores are generated from many available sources of **subjective and objective data** including external benchmarks, our experience, client history and qualitative and quantitative analysis	• The availability of “good” data on controls **impacts the quality** of the analysis; additional data gathering through “crowdsourcing” and other polling methods can make a big difference
• **Automated controls** tend to have higher *operational* scores but lower *flexibility* scores	• An over-reliance on automated controls, while cost-effective, can **limit adaptability** in the internal control structure
• Supervisory-type controls (e.g. management review) can be provide broad coverage and increase flexibility while **empowering process owners** to manage risk	• In order to internalize effective, quantitative-driven risk management into the IT organization, some number of supervisory controls must **always be in place**
• People-based controls have higher ongoing costs but are **relatively easy to design and implement**; the operating costs of automated controls **approach zero** but there are non-trivial costs associated with the design and implementation of the controls	• Both on-going operational costs and one-time design/implementation costs should be understood to ensure that a **true cost picture** is presented

This information is confidential and was prepared by ControlMetric solely for the use of our client; it is not to be relied on by any 3rd party without ControlMetric’s prior written consent.

Rank order model produces risk-control plot

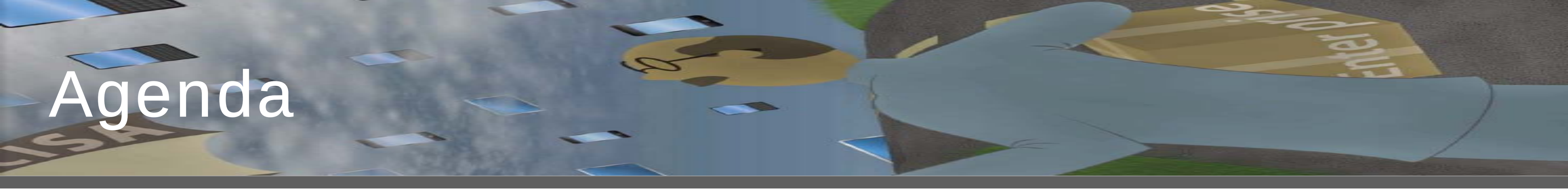


Recommend any changes or additions to implemented controls



Subset	*Controls*	*Residual Risk*	*Cost*	*Overlap to Existing Controls*	*Difficulty of Implementation*
A36	3,4,7,11,15	$9,750,000	$425,000	High	Medium
A17	1,5,6,8,9	$8,500,000	$420,000	High	Low
D14	3,5,8,12,20,21	$4,750,000	$405,000	Medium	Low
B71	1,5,8,11,21	$4,600,000	$460,000	Medium	Medium
C65	1,3,6,8,9,11,13,14,21,22	$4,450,000	$505,000	Medium	High

The final choice of controls includes a subjective review of these criteria

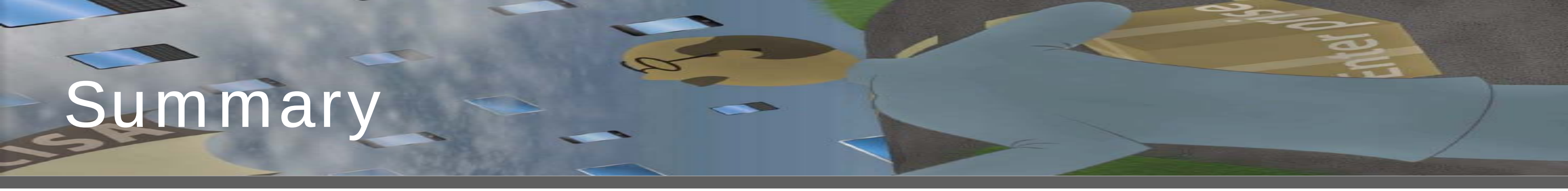


Agenda

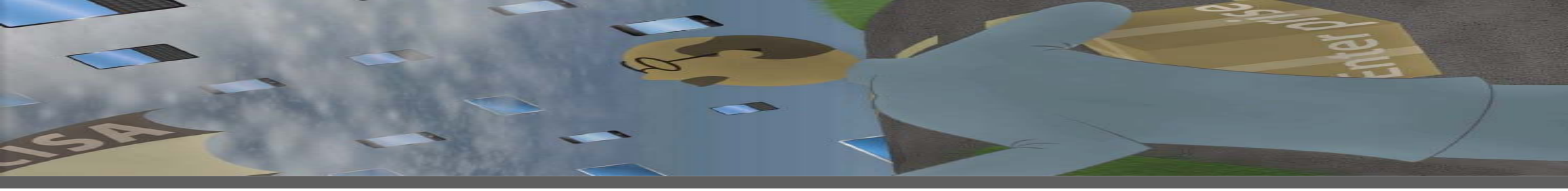
- Introduction
- Estimating the size of risk
- Measuring the mitigation effect of controls
- Summary/wrap up

This information is confidential and was prepared by ControlMetric solely for the use of our client; it is not to be relied on by any 3rd party without ControlMetric's prior written consent.

Summary



- Managing operational risks adds **layers of complexity and associated costs** to business processes, yet many companies find it difficult to assess how much risk is mitigated by their choice of controls
- Quantifying risks and controls develops a **rigorous, defensible view** on the operational risks facing the business, and the ability of a group of controls to mitigate risk in a business or IT process
- Business and IT process owners benefit from the knowledge that selected internal controls will **mitigate the appropriate level of risk** based on their design



ControlMetric

THE SCIENCE OF INTERNAL CONTROL™