

Addressing SOx Risks in an Enterprise Risk Management Process (ERMP) Environment

CEAA Conference
October 6, 2005





The Enterprise Risk Management Process (ERMP)

What Is ERMP?

*Looking across all of
Falconbridge Limited*

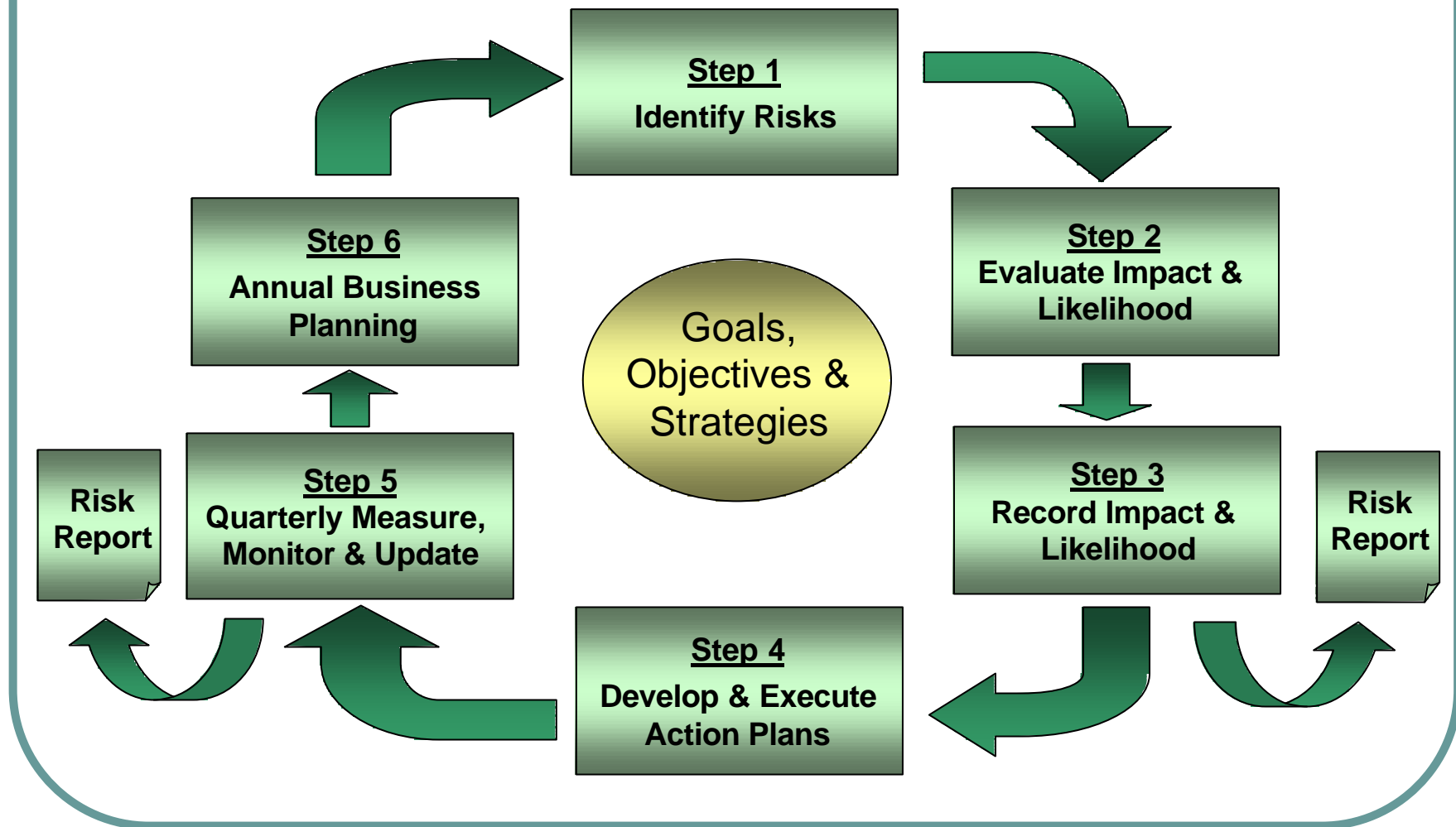
*Something that can
get in the way of us
achieving our
objectives*

**Enterprise Risk
Management Process**

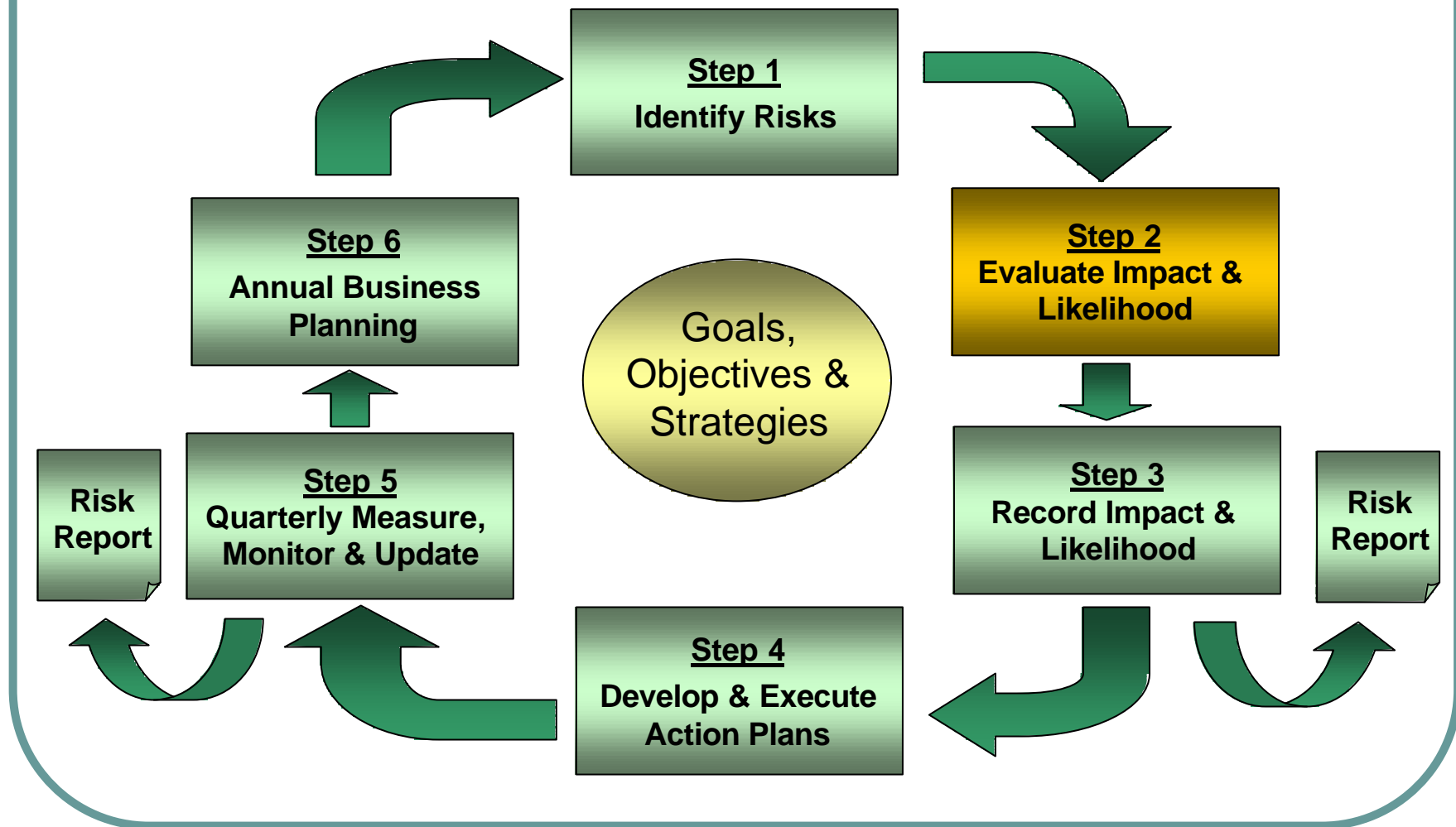
Why Implement an ERMP?

- Regulatory requirements demand a documented, controlled and measured enterprise-wide business process.
 - Sarbanes-Oxley in the U.S.A.
 - Ontario Securities legislation
 - Public disclosure case law
- Management focused on ways to identify and capitalize on risk opportunities.
 - Can we improve on the way that we manage risks?
 - Can we improve on our capabilities?
 - Can we improve on our understanding?

What Is The ERM Process?

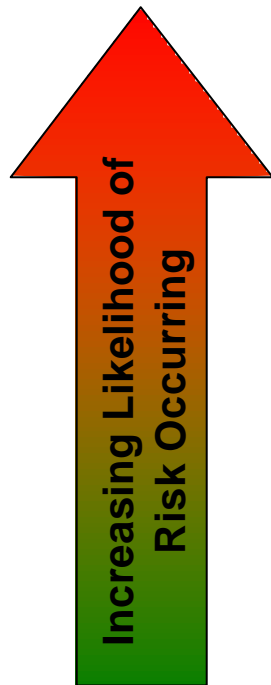


How Is Step 2 Accomplished?



How Are Impact & Likelihood Evaluated?

Increasing Likelihood of
Risk Occurring

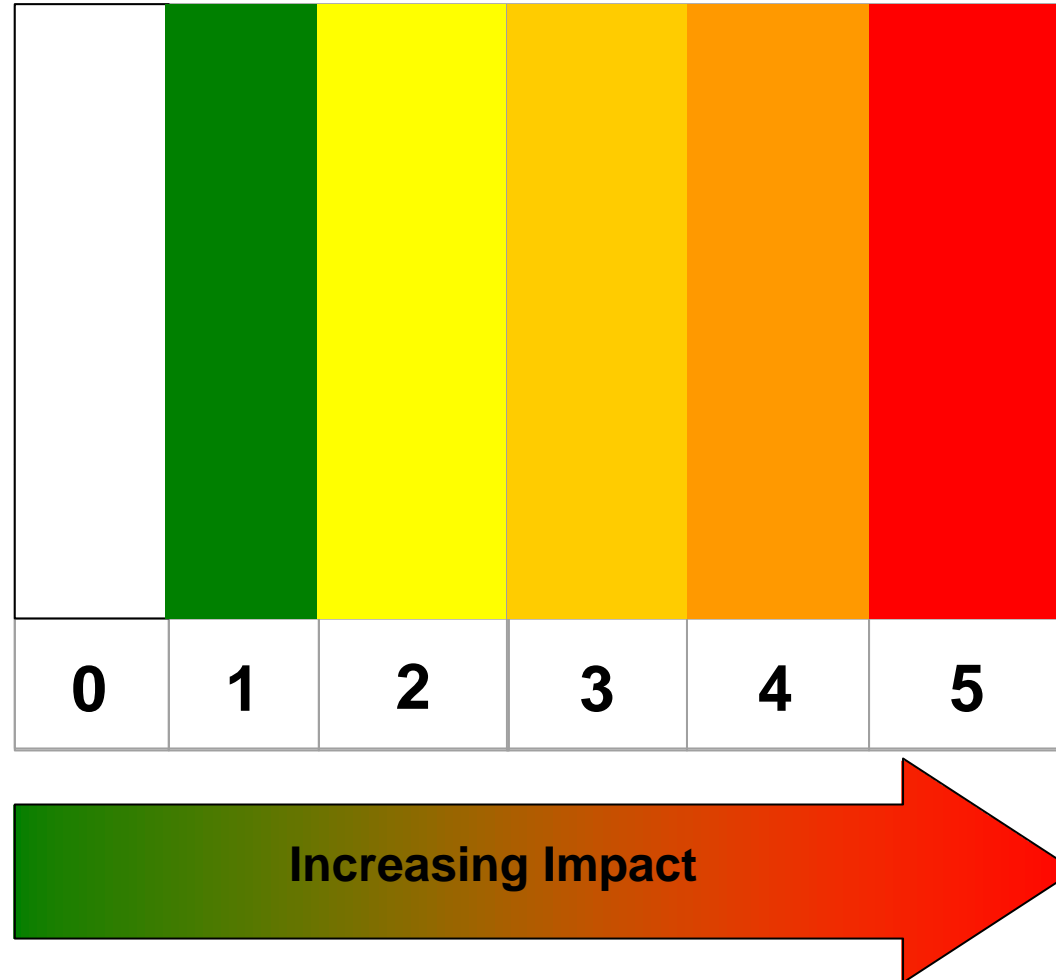


Increasing Impact

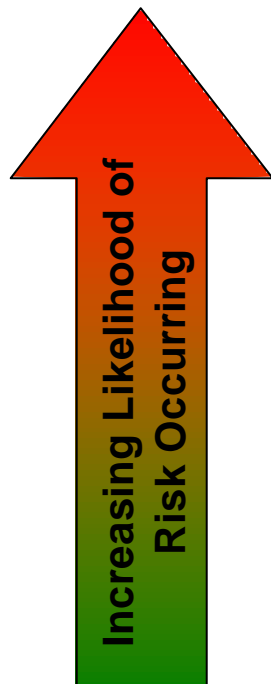


How Is Impact Evaluated?

Defined levels to indicate the “degree of pain” to be assigned to each category of risk being evaluated (ie market risk, health & safety risk, financial risk, etc)



How Is Likelihood Evaluated?



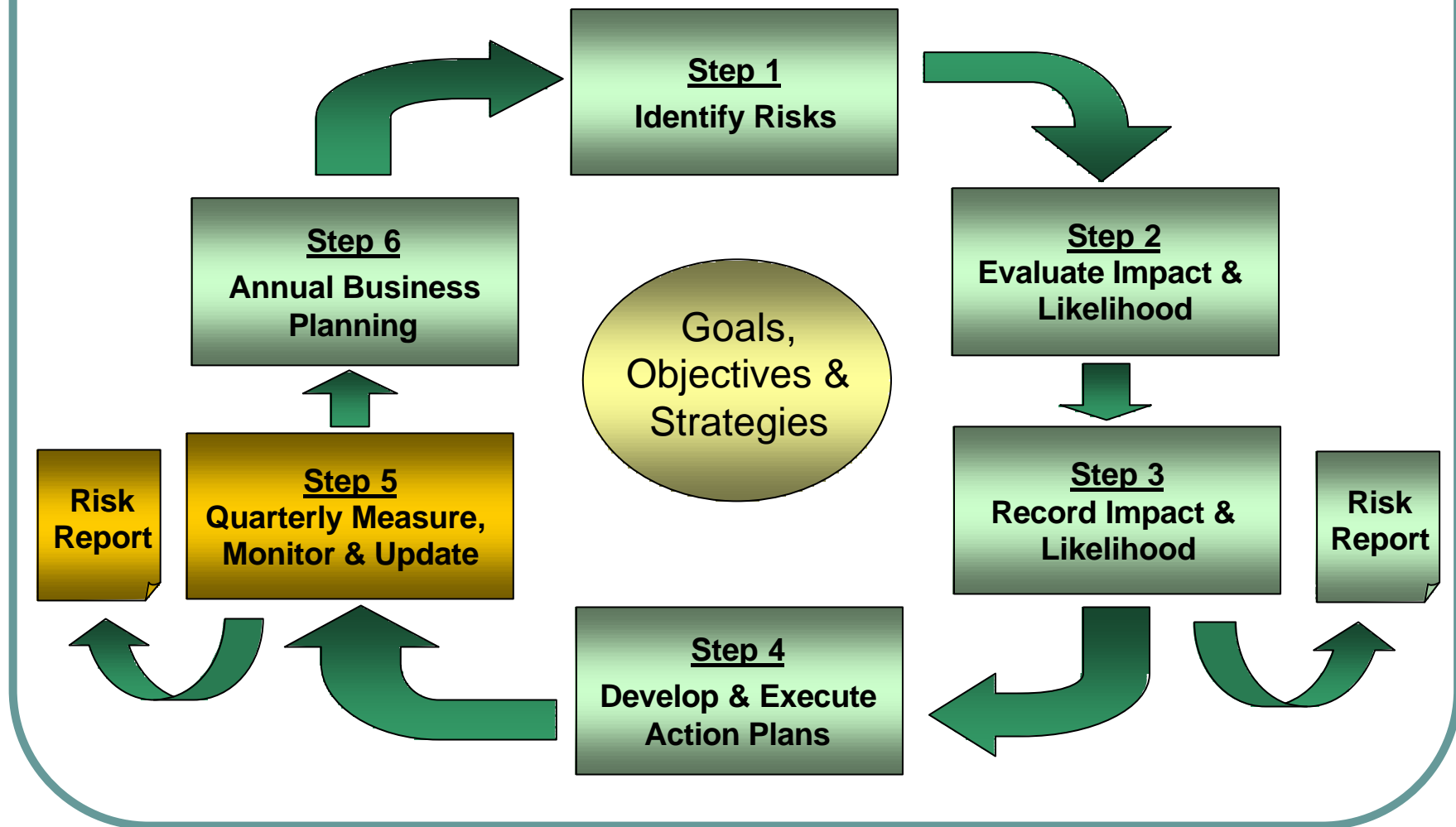
4	Expected to occur more than once a year; chance of occurring is more than 50% in current year; will definitely occur at some time				
3	Expected to occur less than once a year; chance of occurring is less than 50% in current year; will probably occur at some time				
2	Expected to occur less than once every 20 years; chance of occurring is less than 5% in current year; could occur at some time				
1	Expected to occur less than once every 100 years; chance of occurring is less than 1% in current year; occurs in exceptional circumstances				

What Is The Risk Level?

**Overall risk level
of each risk is
determined
based on the
Likelihood and
the Impact
assigned**

4					
3					
2					
1					
	1	2	3	4	5

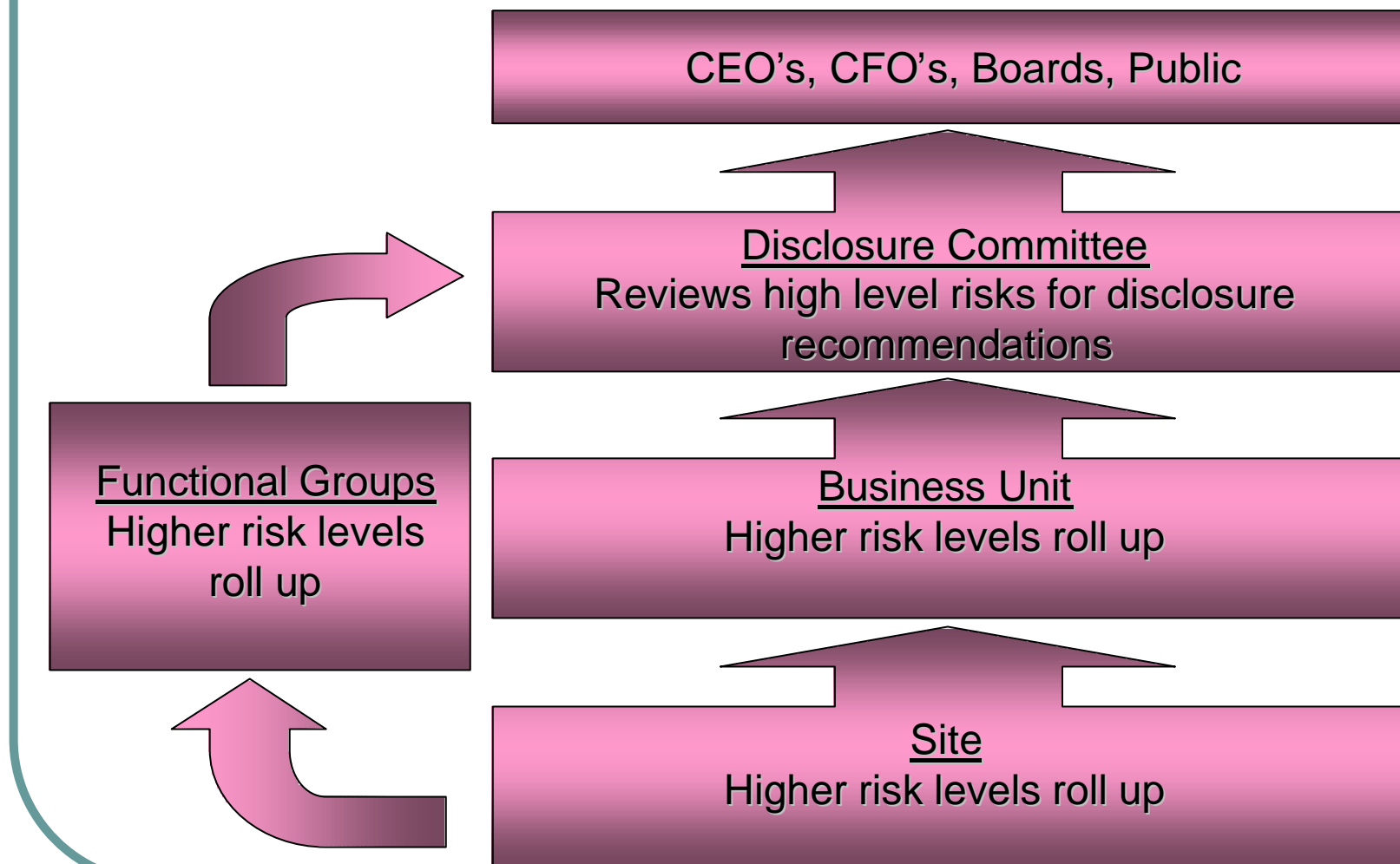
What Is Involved In Step 5?



What Is The Quarterly Risk Report?

- Quarterly risk report contains:
 - addition of new risks / deletion of previously existing risks now being sufficiently managed
 - updated risk levels for previously existing risks
 - risk level trending from previous to current quarters
 - updated actions and responsibilities for managing risks

What Is 'Reporting Rollup'?



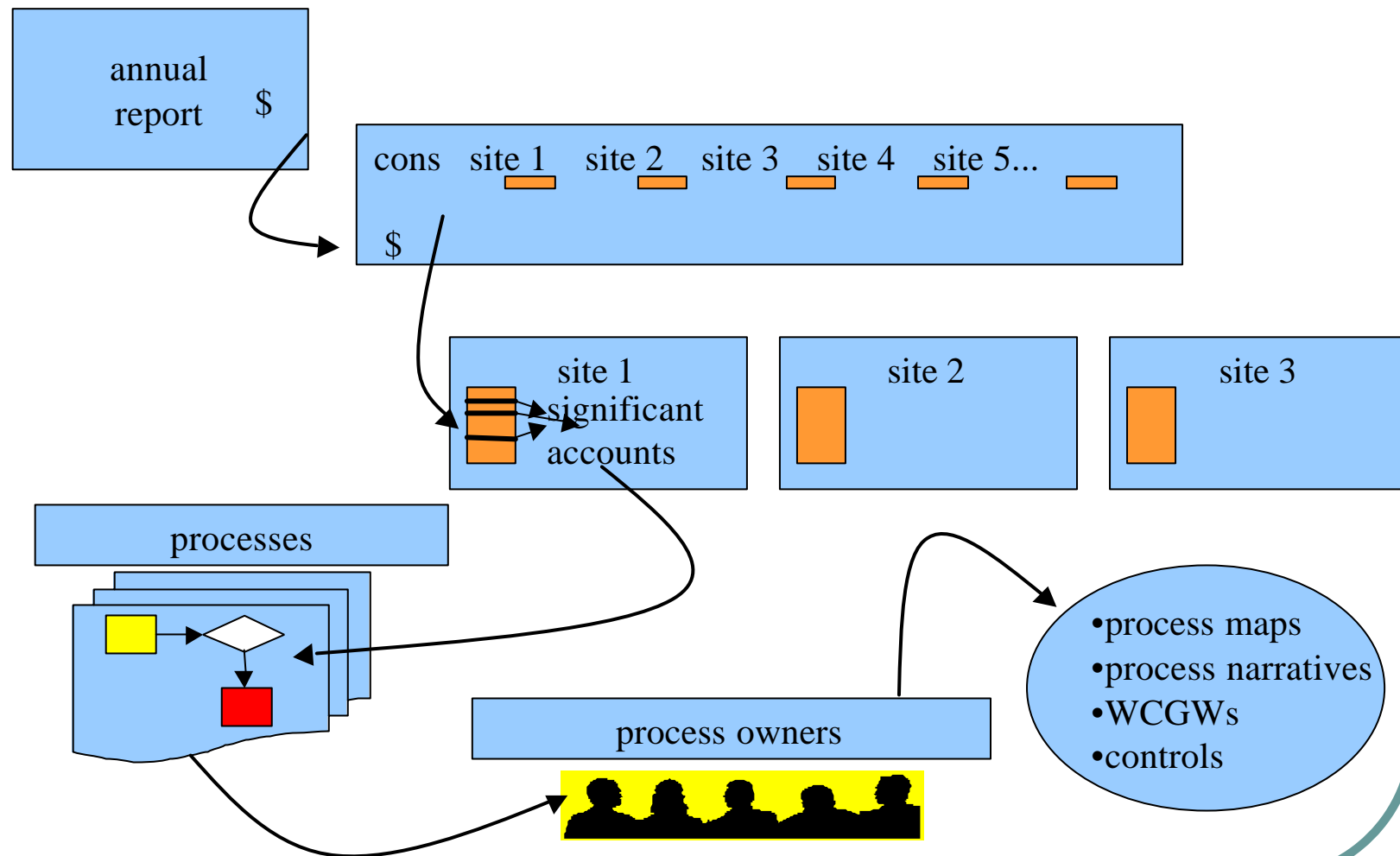


Documenting Internal Controls over Financial Reporting (SOx)

What Is One Methodology For SOx?

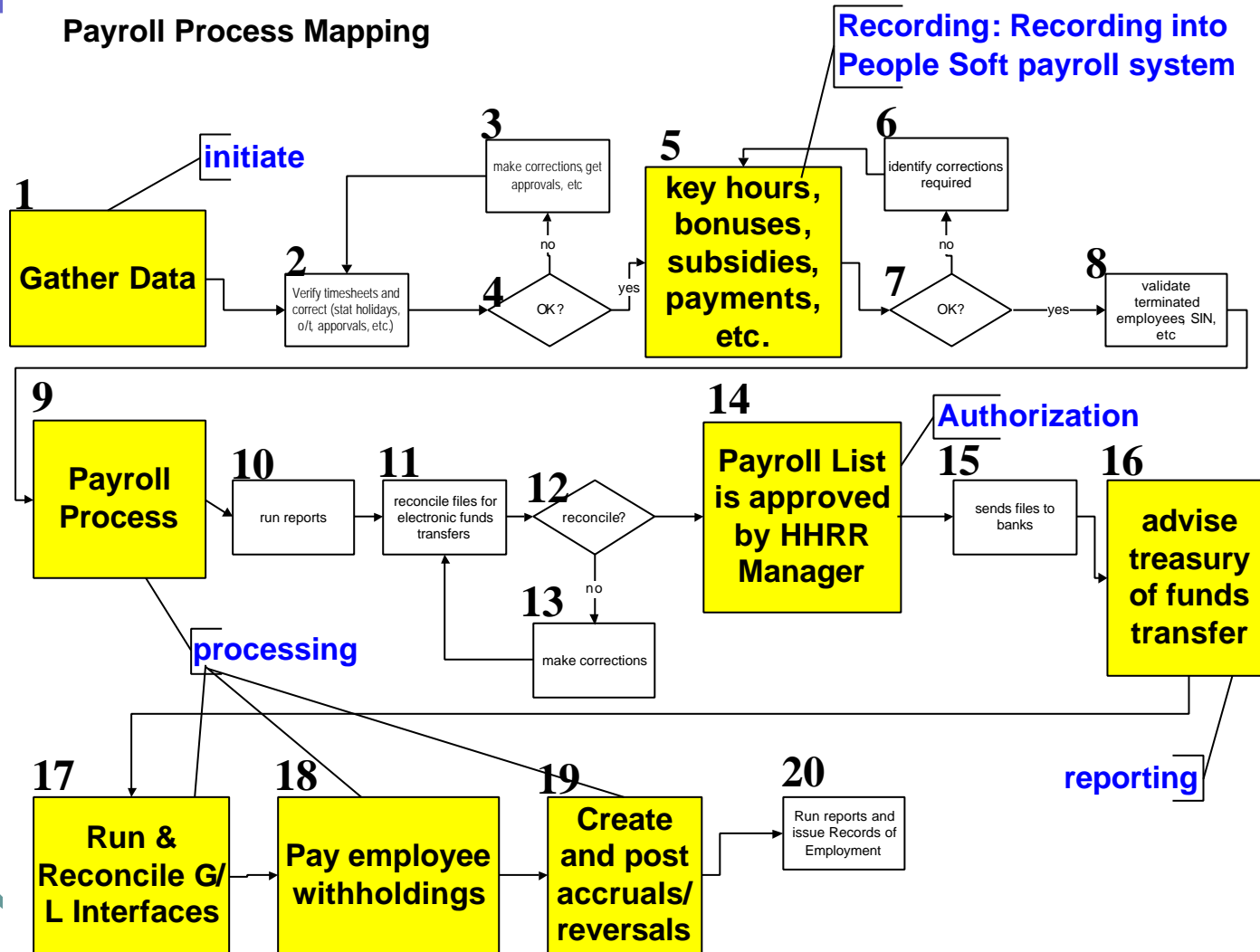
- Ernst & Young annual process
 - Begin with the annual report for previous year
 - Break down into general ledgers, BUs and sites
 - Select accounts that are 'significant'
 - Identify processes that populate accounts with \$
 - Document process maps & narratives
 - Identify 'what-could-go-wrongs' (at critical activities)
 - Document controls that either prevent things from going wrong, or detect when they do
 - Test controls to ensure that they are working effectively
 - Remediate where necessary

What Is The E&Y Methodology?



What Is A Process Map?

Payroll Process Mapping



What Are Critical Activities?

- ❖ initiation
- ❖ recording
- ❖ authorization
- ❖ processing
- ❖ reporting

What Is A Process Narrative?

Example narrative for the 'payroll process'

Step 1 – gather data. The paymaster ensures that all timesheets are gathered on a bi-weekly basis. The timesheet is a heavy stock paper product, completed in ink by the employee and duly approved by the employee's supervisor. The supervisors send these to the payroll department through the inter-departmental mail by one day after the end of the payroll period.

Step 2 – verify time. The paymaster manually reviews the timesheets when received on a bi-weekly basis to verify that: a) statutory holidays, sick time, vacation and other absences have been coded correctly, b) all employees are accounted for, and c) supervisors have approved each timesheet for absences and overtime.

Steps 3 & 4 – OK? Make corrections. The paymaster determines if there are errors or omissions which require correcting. Examples of items which may need correcting include: a) timesheet is missing, b) total hours have been added incorrectly, c) no approval by supervisor, etc. The corrective action for each of the above would require the paymaster to: a) request the missing timesheet of the supervisor, b) correct the total hours on the timesheet and inform the supervisor and employee accordingly.....

What Is A WCGW?

- A question that identifies a risk at one of the 5 critical activities
 - What ensures that all transactions for the month have been recorded?
 - What ensures that there are no duplicate transactions recorded?
 - What ensures that transactions are assigned to the appropriate account?

How Is WCGW Likelihood Evaluated?

Likelihood

probable

**the future event or events
are likely to occur**

**reasonably
possible**

**the chance of the future event
or events occurring is more than
remote, but less than likely**

remote

**the chance of the future event
or events occurring is slight**

How Is WCGW Impact Evaluated?

<p>of <u>no</u> <u>consequence</u> to the financial statements</p>	<p><u>adversely</u> <u>affect(s)</u> the company's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with GAAP</p>	<p><u>material</u> <u>misstatement</u> of the annual or interim financial statements will not be prevented or detected</p>
--	--	--

inconsequential

more than
inconsequential

material

\$ Impact

What Is The WCGW Risk Level?

Likelihood	probable	control deficiency	significant deficiency	material weakness
	reasonably possible	control deficiency	significant deficiency	material weakness
	remote	control deficiency	control deficiency	control deficiency
		inconsequential	more than inconsequential	material
\$ Impact				

What Is A Control?

- A control mitigates a WCGW
- Controls can be:
 - Preventive (preventing a WCGW from happening – ie user name and password)
 - Detective (identifying a WCGW after it has taken place – ie bank reconciliation)
 - Manual (performed by the individual – ie comparison of one month's actual to previous month)
 - Automated (performed by the system – ie same invoice number cannot be processed twice for one vendor)

How Is A Control Tested?

- Test of design (1st test)
 - If design is ineffective, a control may not effectively mitigate the WCGW, even when it is operating as designed (ie one username and password for all users of a system)
 - If test of design fails, control tester does not proceed
- Test of operating effectiveness
 - To be effective the control needs to operate at the assigned frequency without fail
 - Random sample taken to ensure that control operates every time

How Are Control Deficiencies Assessed?

Likelihood	probable	control deficiency	significant deficiency	material weakness
	reasonably possible	control deficiency	significant deficiency	material weakness
	remote	control deficiency	control deficiency	control deficiency
		inconsequential	more than inconsequential	material
\$ Impact				

What SOx Risks Show On ERMP?

Likelihood	probable	control deficiency	significant deficiency	material weakness
	reasonably possible	control deficiency	significant deficiency	material weakness
	remote	control deficiency	control deficiency	control deficiency
		inconsequential	more than inconsequential	material
\$ Impact				

What SOx Risks Show On ERMP?

- potential WCGW risks (ie these have not yet happened)
- actual control risks identified (ie these have happened and are not yet remediated)
 - potential risks growing out of the inability to effectively mitigate a material control weakness (CEO and CFO need to describe material weaknesses – controls cannot be deemed to be effective)