Demystifying Risk Management in ERPs

Liz Piteo, VP Business Development,
Fastpath, Inc.

Professional Techniques – T21

Agenda

- Working together: audit + IT + business process owners
- Approaches to security and segregation of duties analysis
- Understanding systems and system access
- Automation & continuous monitoring

About Me

- Vice President of Business Development of Fastpath, Inc.
- 15 years experience in financial management systems
- Specialize in business process mapping and security configuration

About Fastpath

- 1,000+ customers
- 30+ countries
- 6 continents

Working Together Audit, IT and Business Process Owners (BPOs)

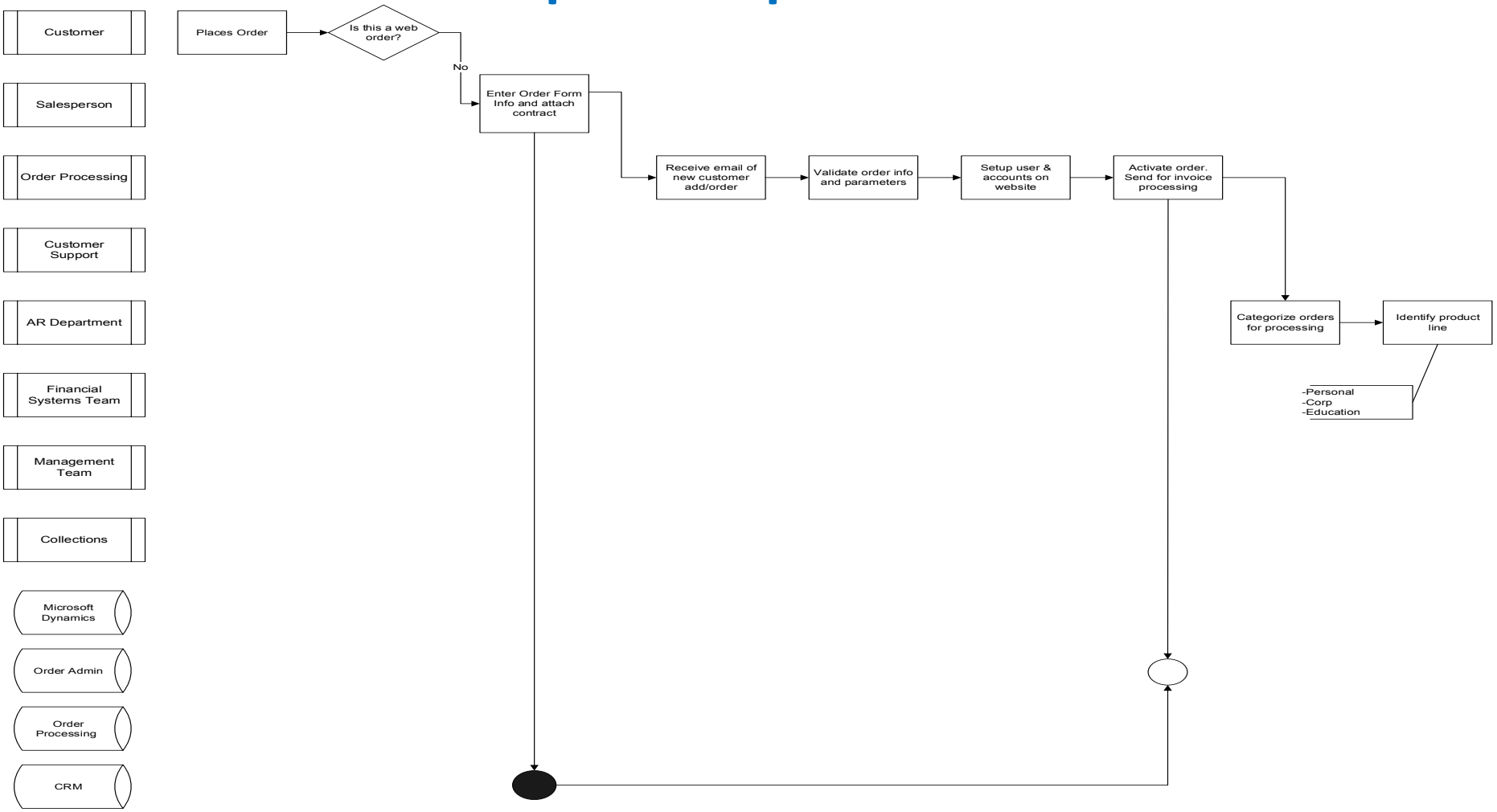
Working Together Audit, IT and BPOs

- ERPs sit in the middle of IT and BPOs
- BPOs unsure of the underlying security
- IT unsure of the business process requirements/risks
- Few people have holistic view of process
  - Processing requirements
  - Financial
  - Roles
  - Systems, data, integrations
  - Risks

Working Together Audit, IT and BPOs

- Identify the processes that are in scope
- Use business process maps to unite the teams
- Involve audit, IT and BPOs in mapping
- Include roles, systems and risks in map
- Provides basis for documentation, training, auditing

Map the process



What we see at our clients

- Access security is low priority for the project team
  - More concerned with getting the ERP set up correctly, business processes put into place
- Process controls are not part of the consideration
  - Sometimes security models are built too stringently when outside controls can be established instead
- Security design is the domain of IT/Sys Admin and business is not aware
  - IT/Sys Admin doesn't always have a good understanding of business processes and they should get BPO input
- No on-going monitoring of process controls
  - Things change rapidly in businesses – there shouldn't be a "set it and forget it" mindset

What we see at our clients

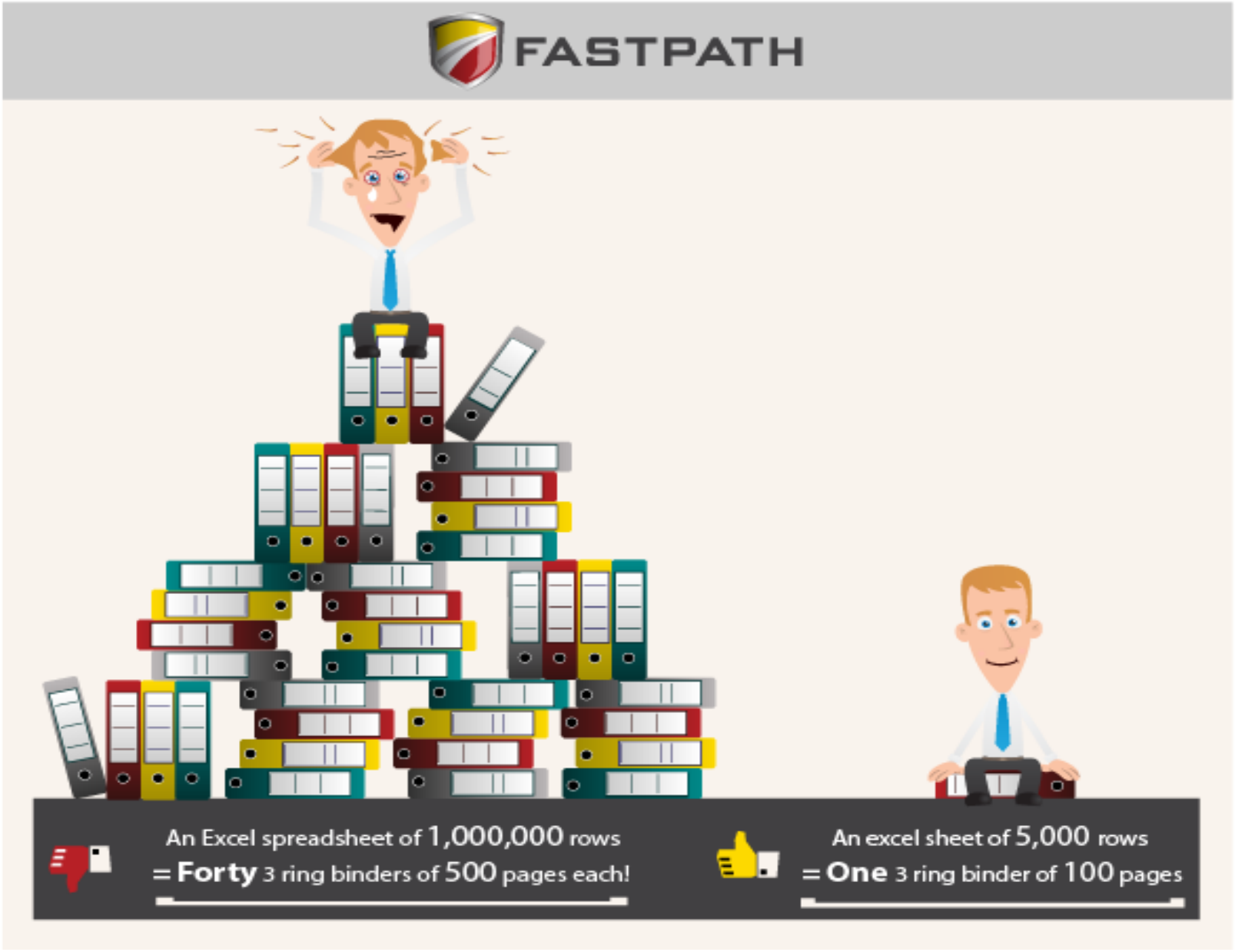
- No consideration of segregation of duties
  - Again trying to build security into each user rather than consider segregation of duties processes, etc
- Dilution of 'go-live' security design
  - Have a great security design at the onset but then it isn't maintained or documented once system is up and running
- Inability to report on current security setup
  - If you have great security but can't run reports against it to prove that security is in place, this can be considered a weakness
- Expensive customizations in place of S&C features
  - Customizations need to be maintained, can be difficult to upgrade, etc

What can you do to be better prepared

ACCESS
Do you know who has it?

CHANGES
Do you know who made them?

RISK
Do you know where you are vulnerable?


FASTPATH
An Excel spreadsheet of 1,000,000 rows
= Forty 3 ring binders of 500 pages each!
An excel sheet of 5,000 rows
= One 3 ring binder of 100 pages

Application Security – Who has access?

- Take a risk based approach
- Analyze by function not by user or risk
- Average system has over 5000 access points
- Average system has 30-40 high risk access points
- 500 vs. 1,000,000
- Reviews performed by BPOs not IT

Application Security – Who has access?

Customers
Vendors
Item/Inventory
Pricing
HR
Payroll
Process disbursements (check run)
Release/Approve purchase order
Goods receipt
Enter vendor invoices
Post journal entries
Open/Close GL accounts
Ship customer orders

Accounts Receivable transactions (post cash, credits)
Credit & Collection (credit limits, hold, release)
Customer order entry
Process/Modify customer invoices
Process credit memos
Write-off customer accounts
Record labor hours
Payroll payment (check run)
Prepare payroll (calculation/approval)
Open/Close Fiscal Periods
Maintain Users/User Security Privileges
System/ Module Configuration - Settings

Examples of risk from application security

- Having ability to create a vendor and pay a vendor
- Having ability to create/modify payment terms and create modify vendors/customers
- Having ability to transfer inventory and change stock counts
- Having ability to create purchase orders and receive goods

System access – Administrative Access

- What functions are required for admin
- Maintenance, code release, upgrades, security
- System admin role – how does it work?
  - Programmatic
  - Alternative – assign necessary (all?) roles to user
- Use named users with admin role
- Consultants use
- Periodic reviews

Application vs. Database Security

- How are they integrated
- How are changes made at the database level?
  - Named users vs. Service account
- Periodic reviews
  - Reconcile app and db users
  - Administrative users
  - Custom integrations/outside access

Segregation of Duties

- Preventative vs. productivity
- Build a rule set of potential conflicts
- Identify Conflicts
- Mitigations
- 3 key questions
  - What are your rules?
  - Where are your risks?
  - What are you doing about it?

Audit trails – What did they do with that access?

- Take a risk based approach
  - Focus on key areas – Vendors, configuration, cash receipts, etc.
  - Focus on key fields – Payment terms, addresses, pricing, etc.
- Who changed it?
- When was it changed?
- Was it changed the right way?

Questions

Liz Piteo

liz@gofastpath.com

Twitter: @gofastpath

Questions?

Liz Piteo
liz@gofastpath.com
Twitter: @gofastpath