



A simple approach to

Global I.T. Risk Management

Paul Prentice CISSP | Manager, IT Security, Risk, & Compliance | Steelcase Inc. | +1 616 246 4422
paul.prentice@steelcase.com

we live in a **Complex World**

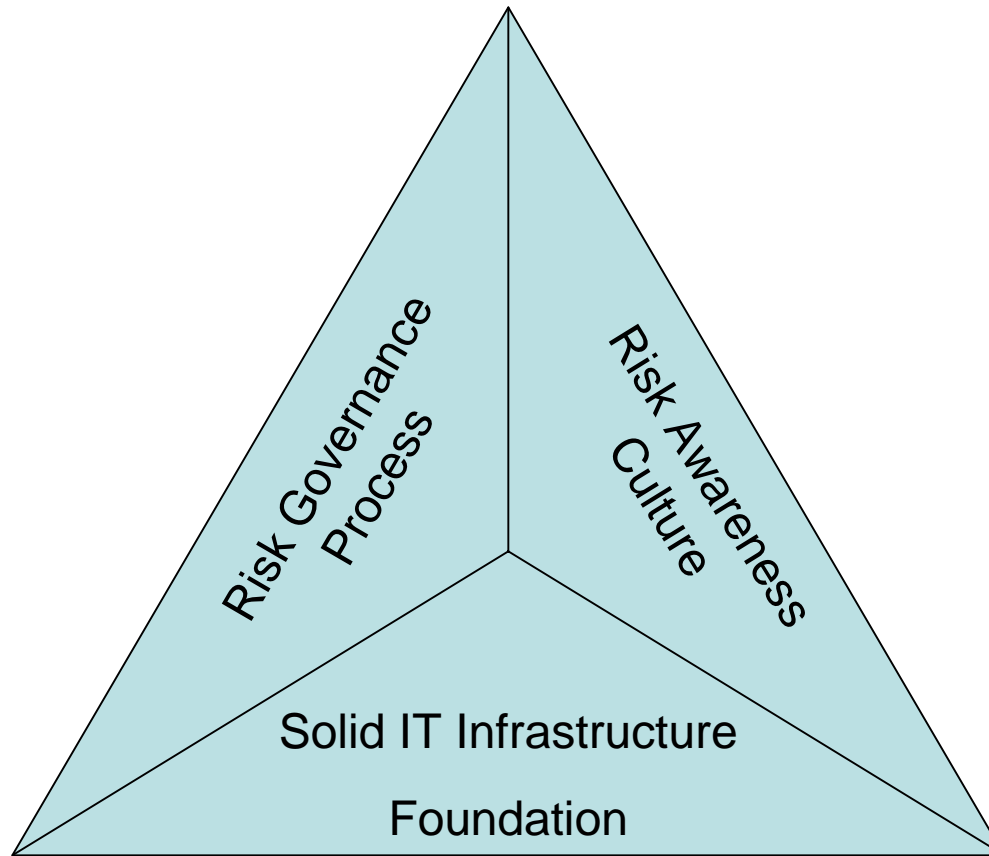
- In the old days, I.T. Life was much simpler
 - ASYNC, BISYNC, ASCII, EBCDIC, & then graduated to SNA, SDLC, PEP
- Now the I.T. world has mushroomed into complexity
 - DNS, DMZ, VPN, PPP, L2TP, PPTP, TLS, SSL, CA, PKI, IPS, IDS, CISSP, SNMP, SMTP, OSPF, WEP, WPA, DHCP, DSL, HTTP, 3DES, NAT, DDoS.....
- The Audit world isn't much better
 - COBIT, COSO, CISA, CISM, ISACA, SOX, ITAF, CGEIT, CACS, ITGI, IFAC, IAASB, ISA, AICPA, ISAE, NIST, SOX, VALIT.....
 - Here's a couple more to add to the list...
 - B.L.T.N.T. (BLT Not Toasted), S.O.B. (Soggy On Bottom), S.H.I.T. (Should Have had It Toasted)

the Approach

- Did some research w/Gartner, IEC, the Web, risk mgmt book
- Created P.O.V. document
 - Added a lot of “credibility” to the process
 - Helped others understand - Why do we need Risk Mgmt?
- Reviewed with Enterprise Risk manager
- Presented the P.O.V. to several I.T. groups
- Defined a “Risk Ratings” document to prioritize Business Impact & Likelihood of Occurrence
- Built a “Risk Map” document
- Defined a “Risk Response Plans” document
- Started using the defined process for quarterly updates/reviews

key points from **the P.O.V.**

- I.T. Risks not clearly identified
- No connection with Enterprise Risk
- No consistent prioritization of I.T. Risks
 - Stops the urgent Pop-Ups
- No framework to manage I.T. Risks
- No regional or global focus
- No way to communicate & relate I.T. Risks
 - No real “awareness” of risk mgmt
- Need to fold into Enterprise Risk Mgmt
 - Quarterly Updates to Board of Directors
- Plug for M-Design - **Michele (Most) Schaafsma**
 - **michele@mdesignltd.com**



















From the book **“IT Risk – Turning Business Into Competitive Advantage”**

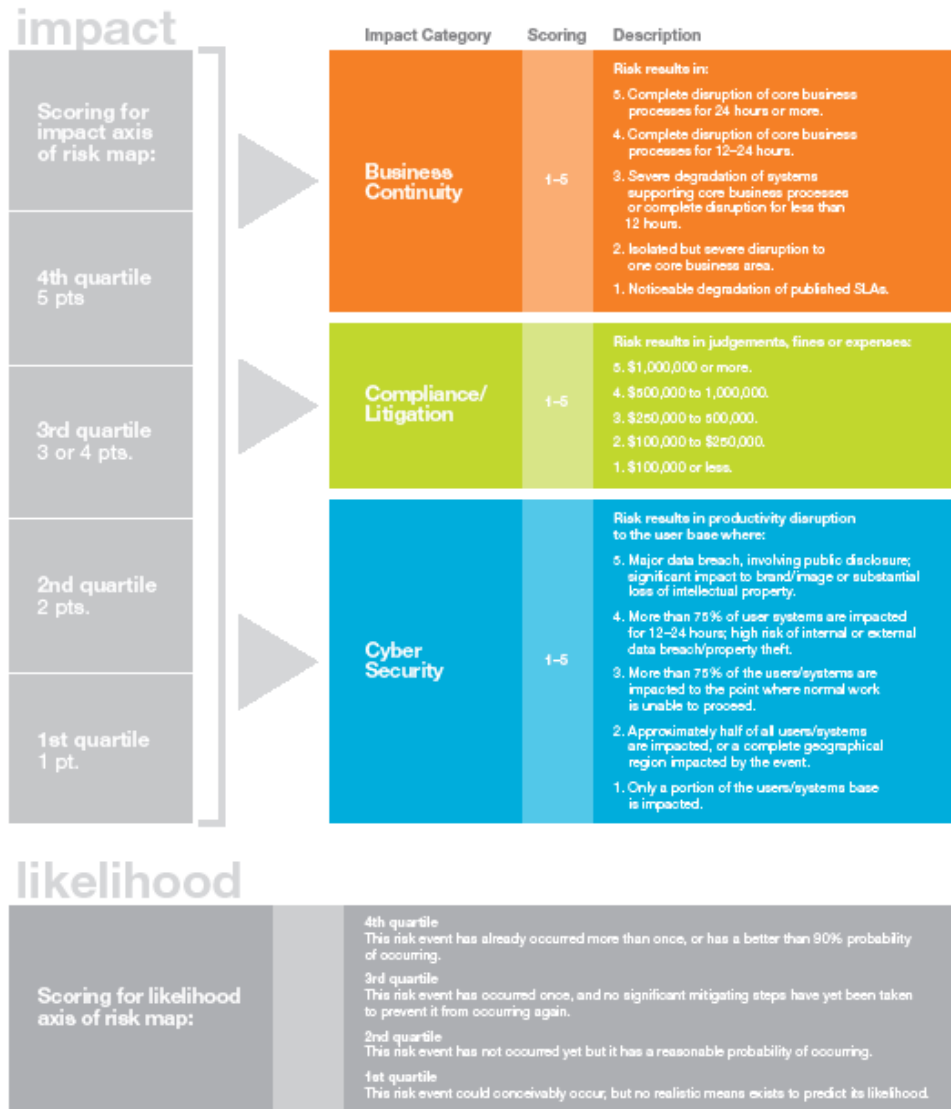
George Westerman – Research Scientist at MIT Sloan School of Mgmt &

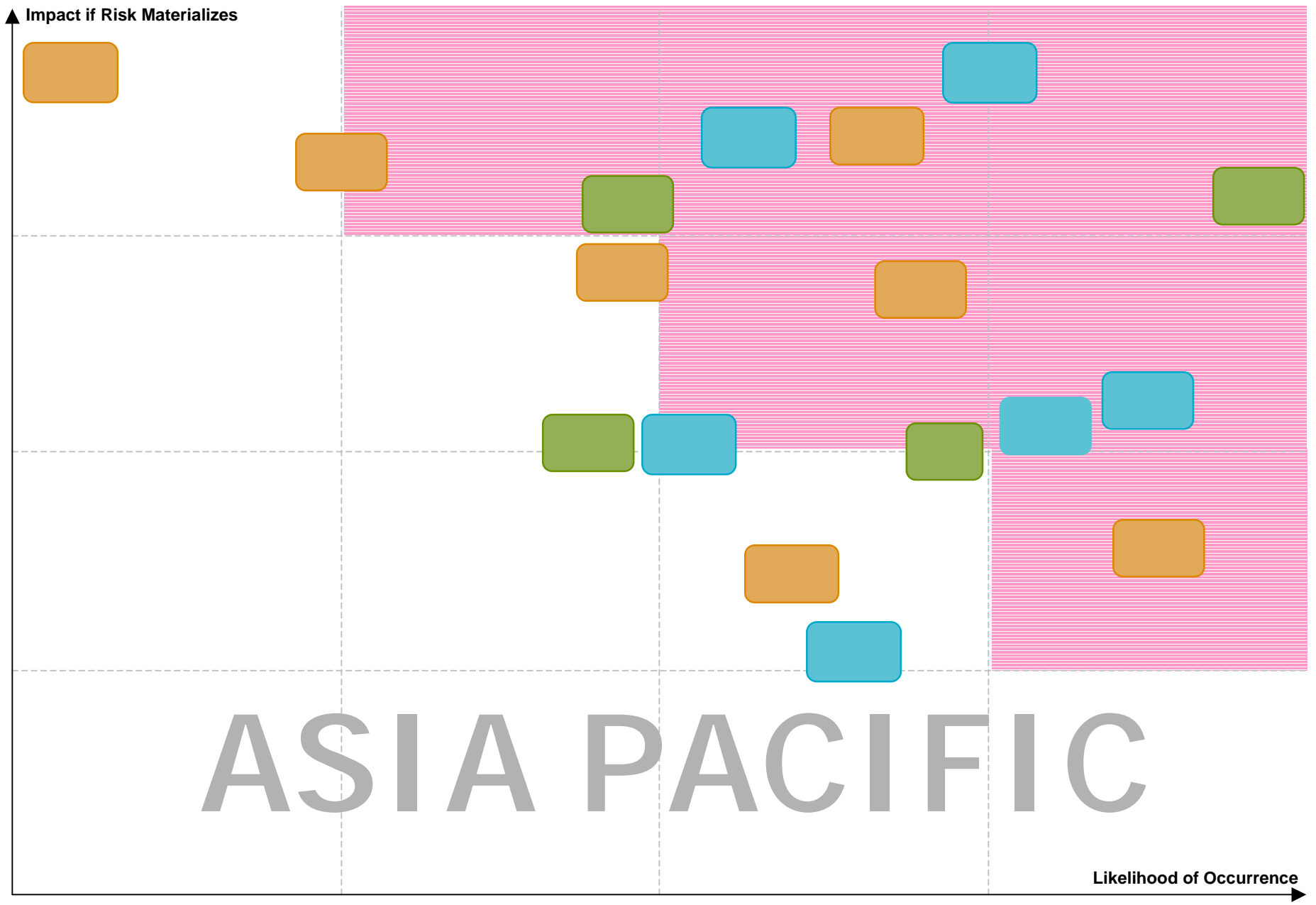
Richard Hunter – VP at Gartner Executive Programs

www.itriskbook.com

Risk	Description of risk	Owner	Current Control (should the risk occur)	Response - Accept, Mitigate, or Transfer (include detailed explanation)	Budgetary Assumptions & Needs	Planned Completion Date
Upper Right Quadrants High/Very High Likelihood, High/Very High Impact 						
						
						
						
						
						
						
						
						
						
						
						
						
						
						
						

Risk Ratings for Business Impact & Likelihood of Occurrence





- Business Continuity** — Interruption of basic business practices
- Legal/Compliance** — Regulatory compliance areas
- Cyber Security** — Intrusion attacks, viruses, spam attacks
- Life/Safety** — Potential life/safety considerations
- * Risk Accepted** — Mitigation too costly; business accepts the risk

QUESTIONS?



A simple approach to

Global I.T. Risk Management

Paul Prentice CISSP | Manager, IT Security, Risk, & Compliance | Steelcase Inc. | +1 616 246 4422
paul.prentice@steelcase.com