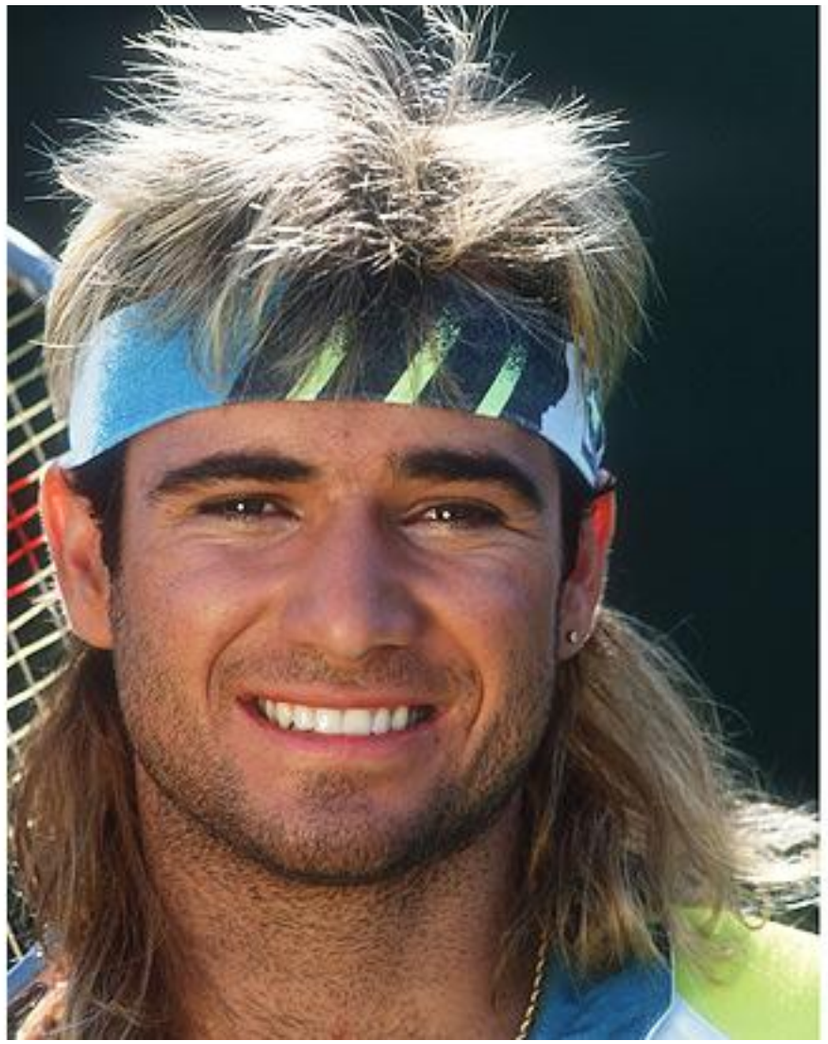
Securing the SDLC for teh Win

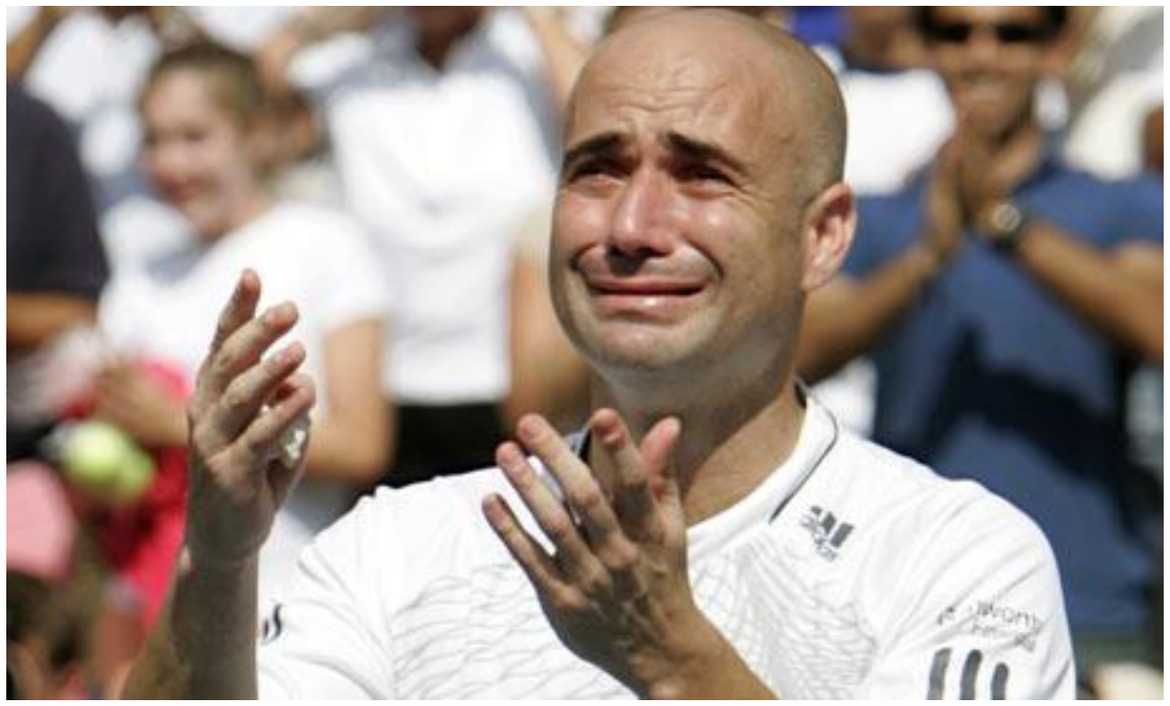
John Melton
Will Stranathan

Faith/Confidence

“Kids, you tried your best and you failed miserably. The lesson is, never try. “

- Homer Simpson





Maturity

“Maturity is achieved when a person accepts life as full of tension.” - Joshua Loth Liebman

“Youth is when you blame all your troubles on your parents; maturity is when you learn that everything is the fault of the younger generation” - Unknown

Sidebar:

Maturity vs. Creativity

"Everything should be made as simple as possible, but not simpler." - Albert Einstein

"What has been will be again,
what has been done will be done
again;
there is nothing new under the
sun."
- The Bible, Ecclesiastes 1:9

“I would rather have my ignorance than another man’s knowledge, because I have so much more of it.” - Mark Twain

“Imitation precedes originality.” - Mary Oliver

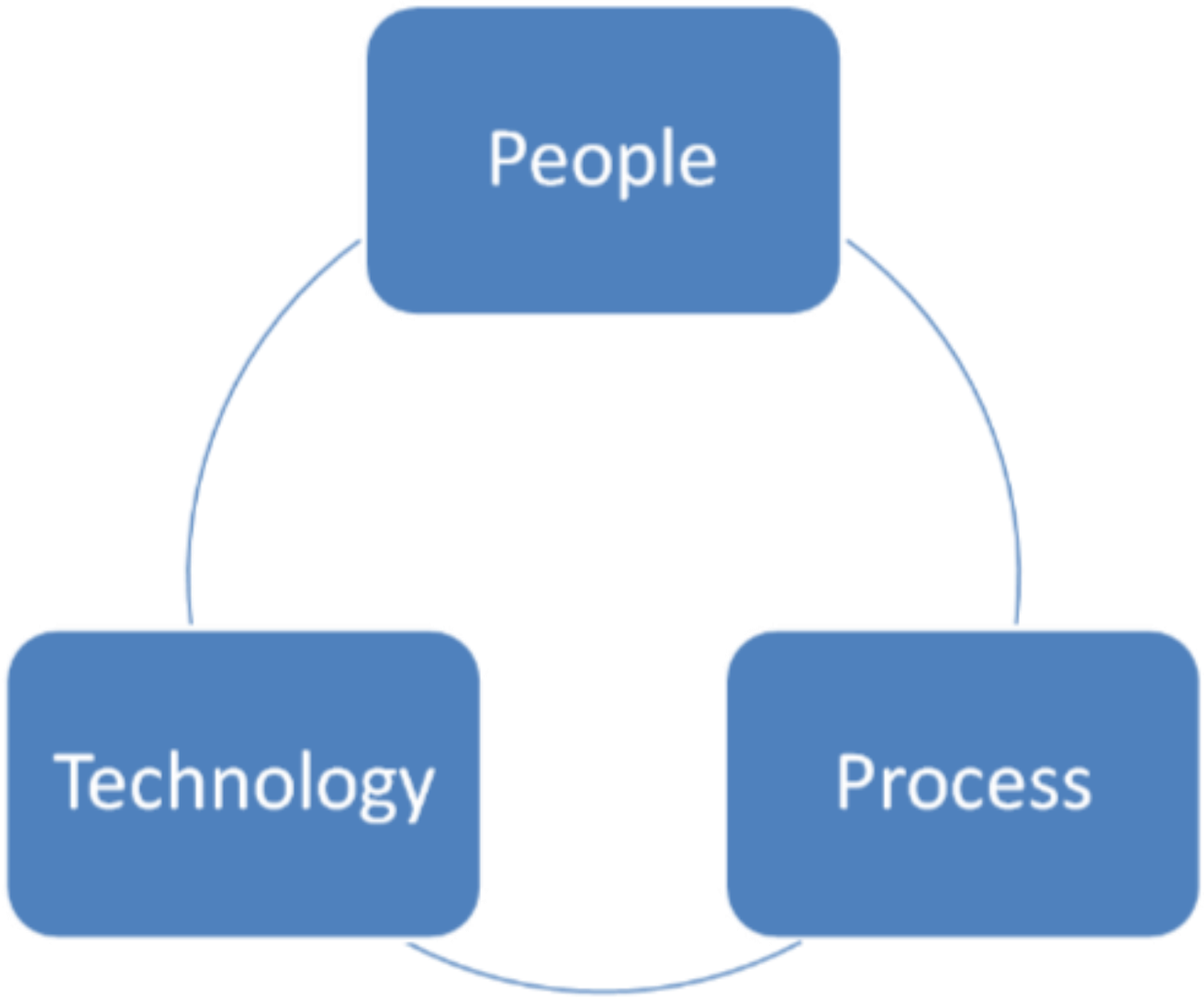
- Adopt

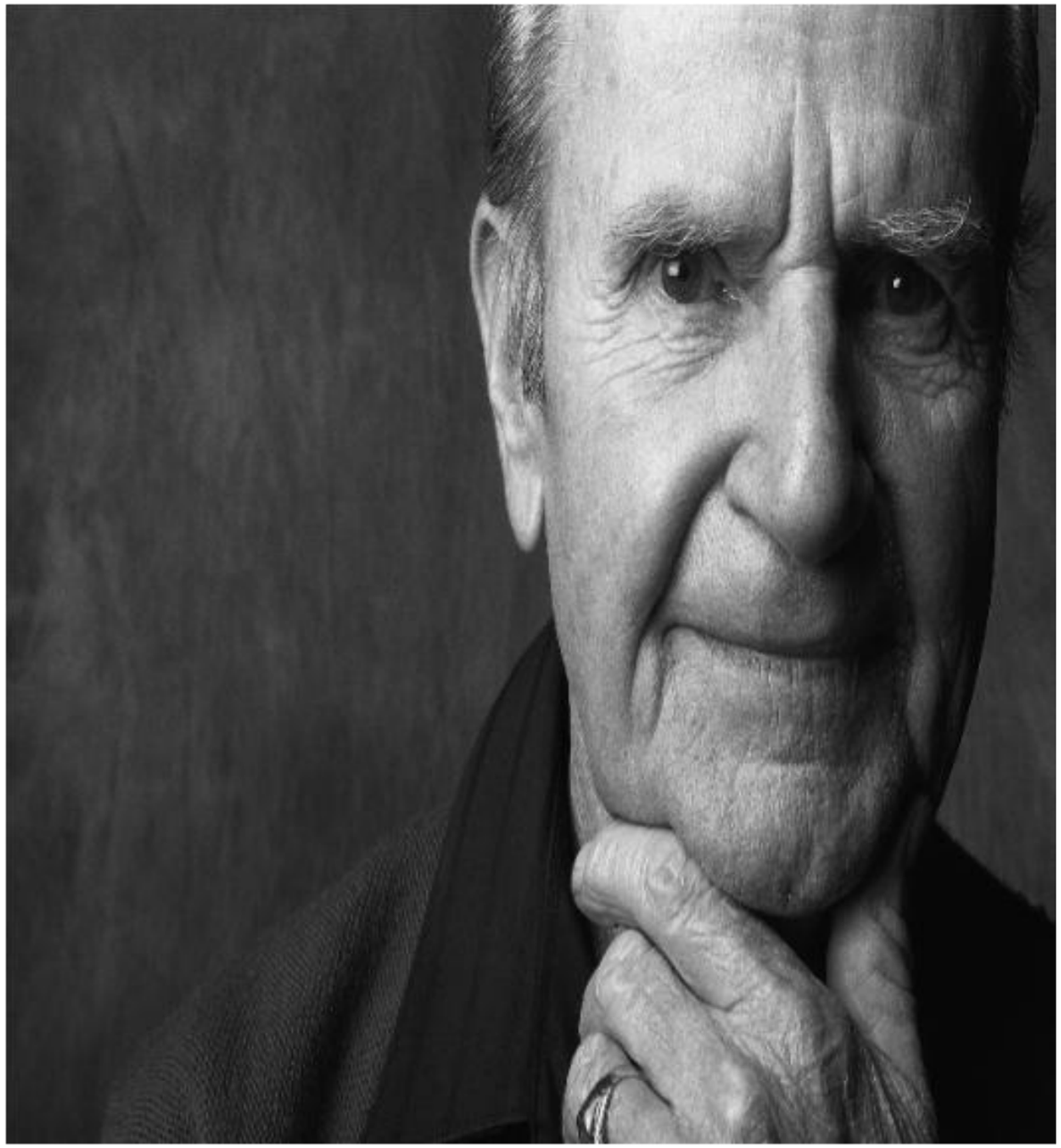
- Adapt

-Adept

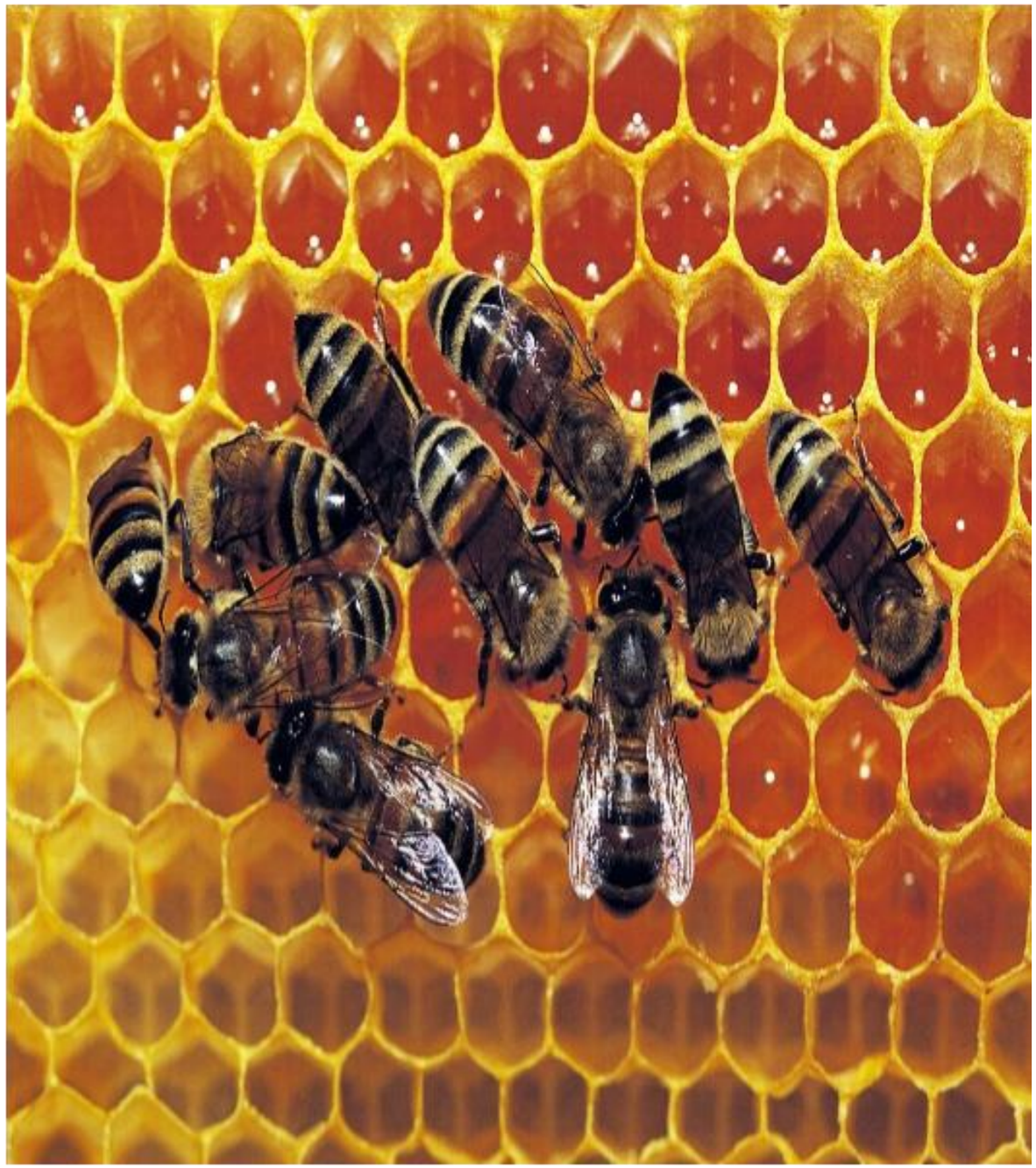
Maturity

Creating Maturity

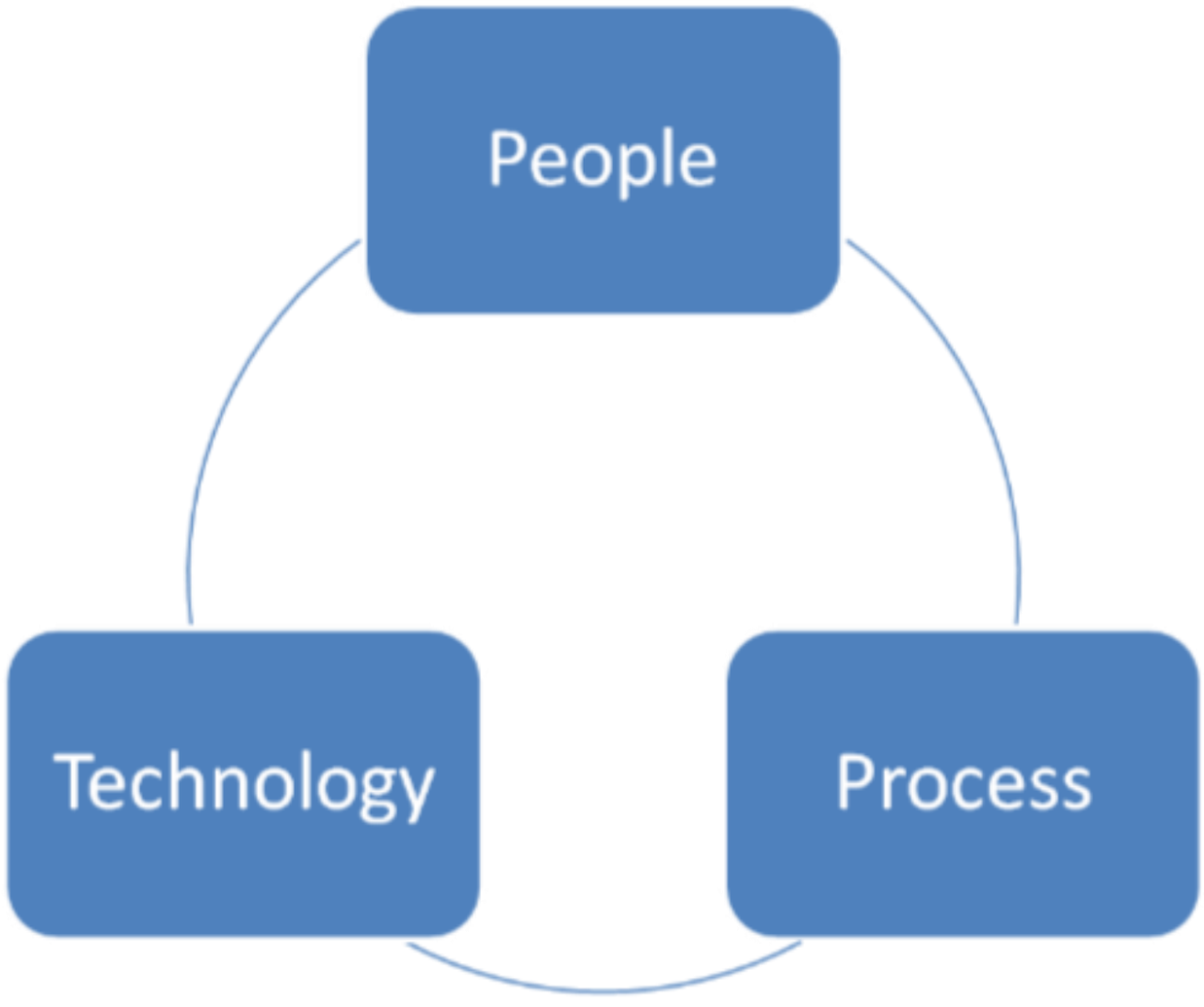





Rapid
A fatal exception 0E has occurred at 0028:C0011E36 in VXD VMM(01) +
00010E36. The current application will be terminated.
* Press any key to terminate the current application.
* Press CTRL+ALT+DEL again to restart your computer. You will
lose any unsaved information in all applications.
Press any key to continue _



People



A Few Ideas

- Books
- Conferences
- Bug of the Month
- Lunch & Learns
- Tie training objectives to performance reviews
- Degree/cert reimbursement
- Internal dev cert program with org-specific info
- Improve hiring process

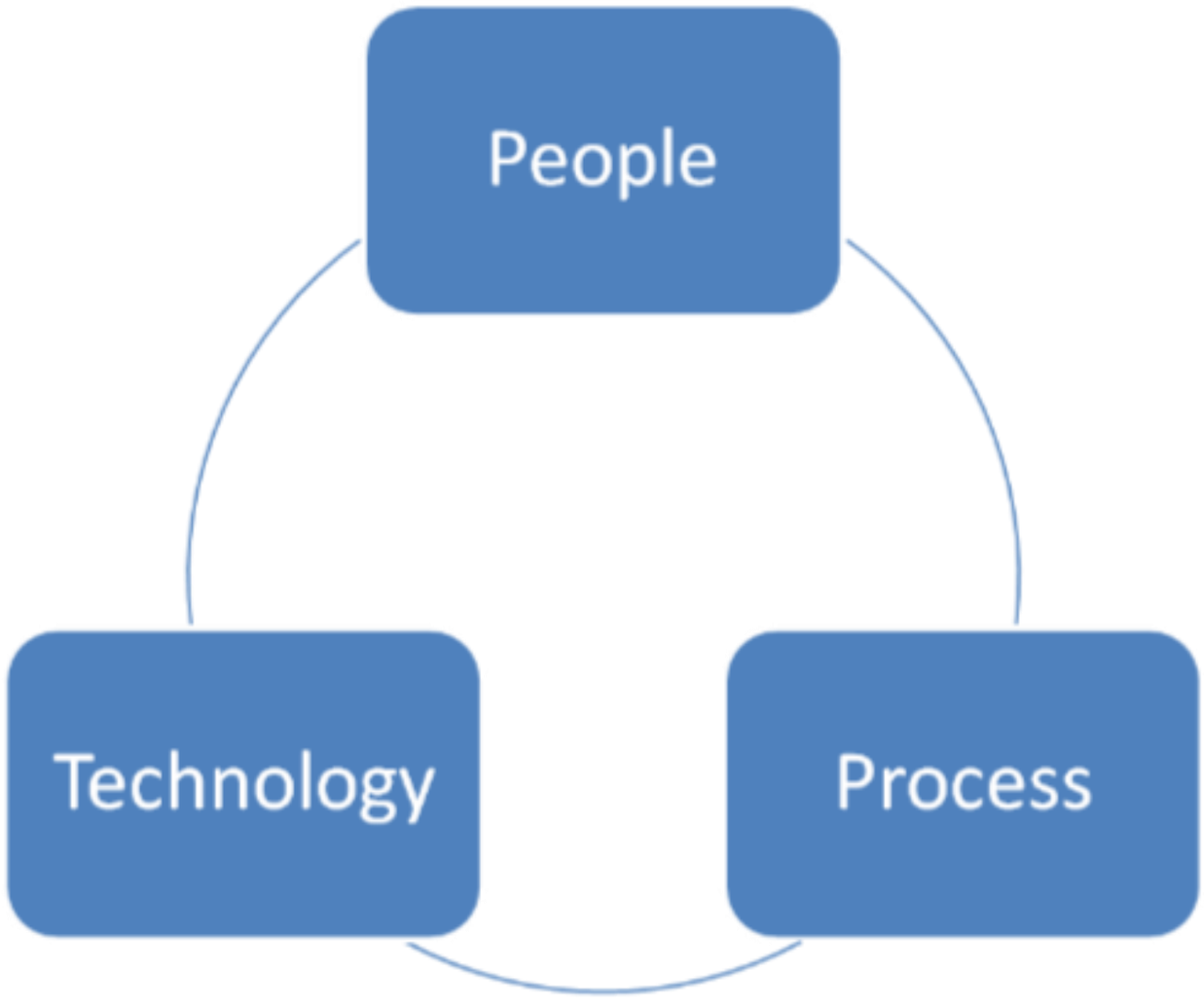
Lunch & Learns

Bug of the Month

Sidebar: Security Echo Chamber

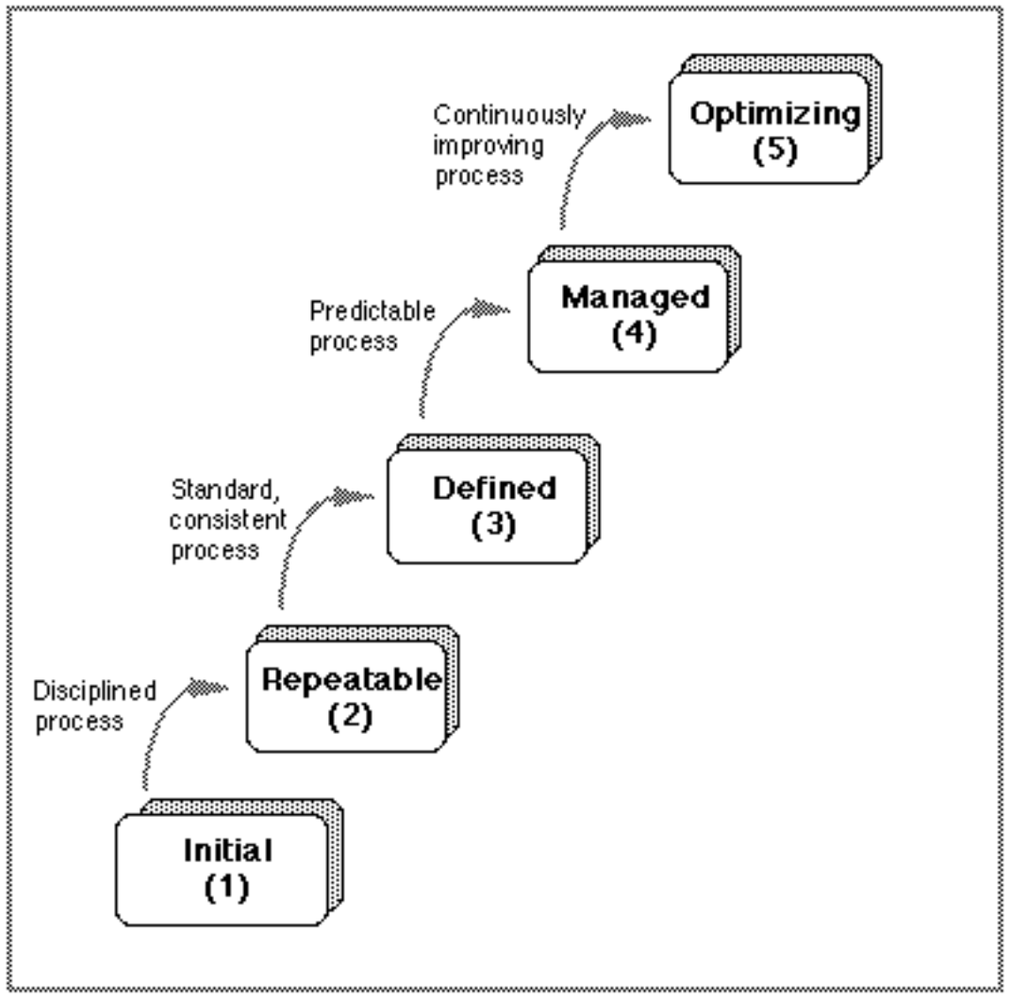
“To me, security is important. But it’s no [more or less] important than everything *else* that is also important!” - Linus Torvalds

Process



Process Maturity

Example: CMM(i)


Continuously
improving
process
Optimizing
(5)
Predictable
process
Managed
(4)
Standard,
consistent
process
Defined
(3)
Disciplined
process
Repeatable
(2)
Initial
(1)

A Few Ideas

- Touchpoints in SDLC
- Thread modeling
- Code / design / architecture reviews
- Treat internal and external code as equally untrusted
- Framework evaluation
- Defined/followed policies for [patching, log review, incident response, remediation, ...]

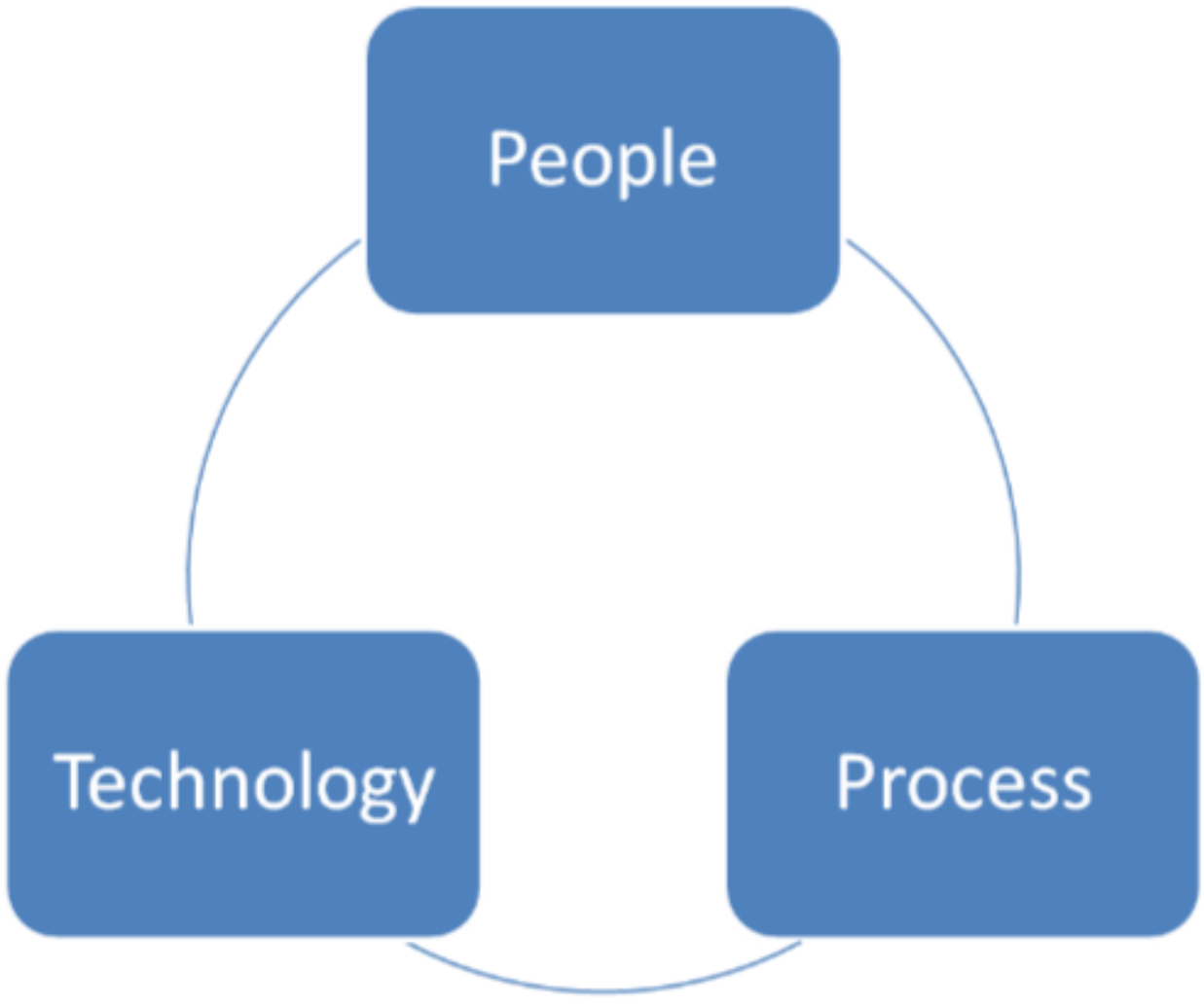
Framework Evaluation

Struts 1, Struts 2, Spring MVC

Trend Analysis

Simple vulnerability metrics

Technology



A Few Ideas

- Static/dynamic testing
- Common security framework (like ESAPI) for organization (and make devs use it)
- Safe(r) languages
- Safe(r) frameworks
- Secure code snippets
- Utilize unit / integration / functional testing to test for security
- Build proprietary tools when necessary

Framework Selection

Struts vs. Servlet/JSP Study

Technology Selection

Twitter / Ruby on Rails

"If you're doing something clever, you're probably doing it wrong"
- Ross Snyder of Etsy

Safe Code Examples / Frameworks

Snippets

ESAPI

Maturity

“Trust everybody, but cut the cards.”

- Unknown

References

- Rugged Software Initiative
  http://ruggedsoftware.org
- BSIMM
  http://bsimm.com/
- OWASP
  http://owasp.org/
- OpenSAMM
  http://opensamm.org
- Microsoft SDL
  http://www.microsoft.com/security/sdl/default.aspx