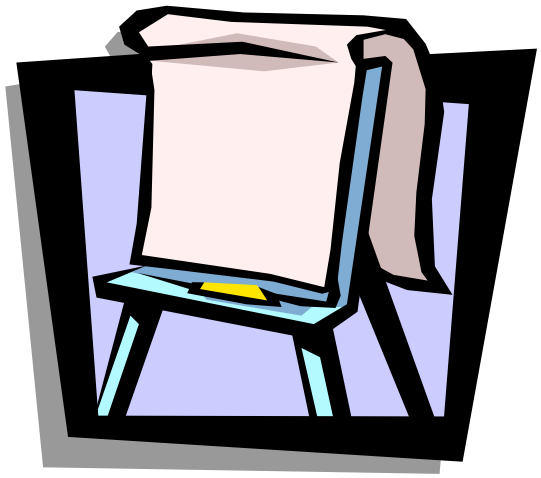
Future-Proof Your Compliance Program

Presented by:
Eric Holmquist
President – Holmquist Advisory
eric@holmquistadvisory.com

Agenda

- Stop the madness - why are we doing this?
- The goal of compliance
- Critical program elements
- Creating flexibility
- Specific topics
- Eyeing the horizon
- Q&A



Why are we doing this?

If your compliance management program is about ticking off a list of controls, you're in big trouble.

Compliance management, as one aspect of risk management, is about risk alignment, not risk elimination, and definitely not about checklists.

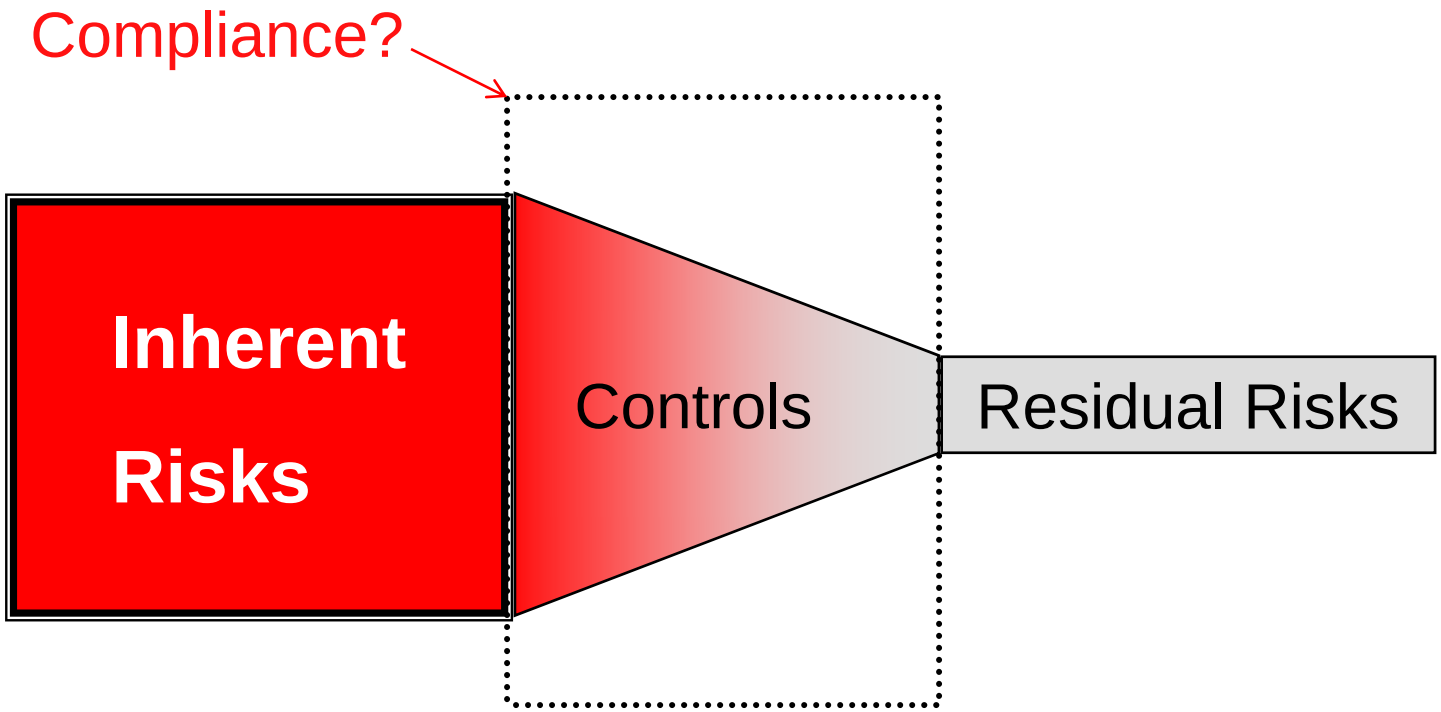
Ultimately risk management comes down to three things:

- **Awareness**
- **Accountability**
- **Action-ability**

Risk Alignment

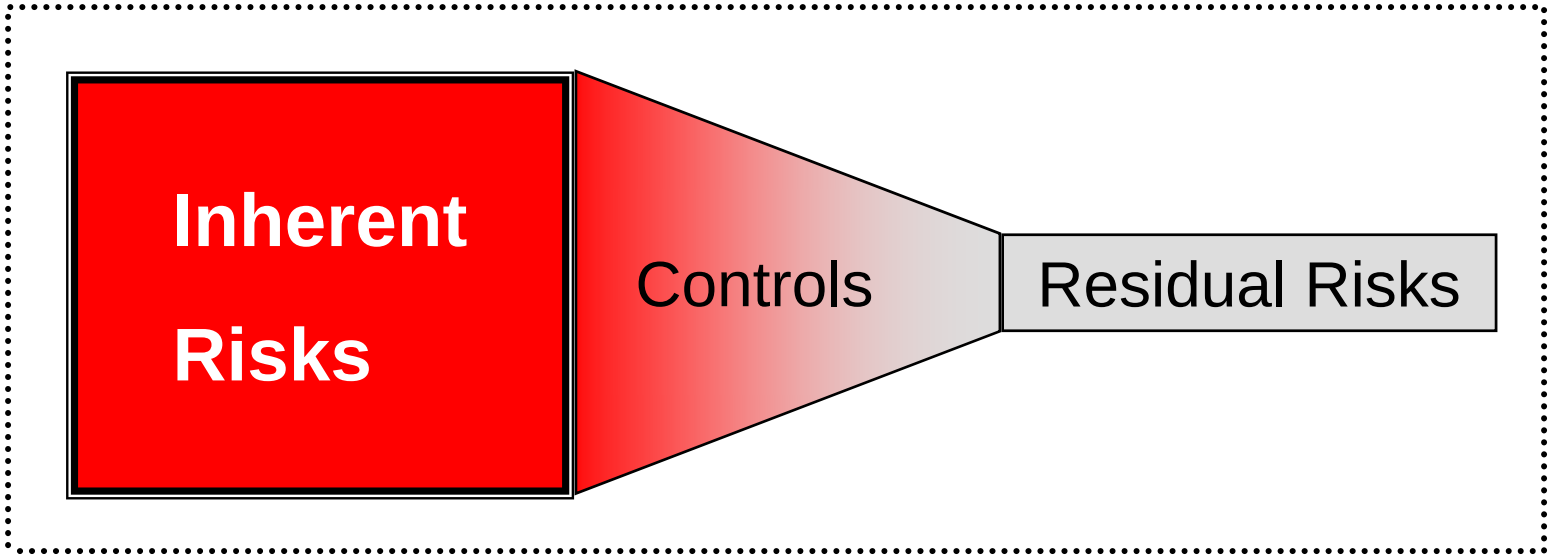
- Mapping guidance to risk
- Mapping risk to controls
- Mapping controls to a process
- Mapping a process to people

The Risk Continuum



The Risk Continuum

Compliance Management!



Key Elements

- Subject matter expert
- Compliance committee (real or virtual)
- Control library – visibility!
- Documentation!!!
- Risk-aware culture
- Incident response team
- Wrap-around analysis

How We Did It

- Never started from scratch
- All new/changed laws/regs mapped first
- Gap analysis against existing controls/reports
- What's required, control or documentation?
- Determined business responsibility
  - Particularly critical for IT based requirements
- Visibility is the key
- Leverage exiting policies, controls & docum.
- Never forget that we have a business to run

GRC?

- Buzzword or not, governance, risk and compliance are inextricably linked
- GRC strength lives and dies on the risk culture
- Requires more end-to-end management
- Compliance is too-often siloed, GRC is holistic
- Compliance must be managed as a part of the risk continuum, NEVER a standalone process

GRC Best Practics

- Executive awareness program should focus on “Are we managing risk?” more than “Are we in compliance?” One follows the other.
  - This means setting risk tolerance
- Executive sponsorship is invaluable
- Strive for end-to-end process maps
- The value of a control library (risk mapping)
- Don’t let everyone’s responsibility become no one’s responsibility

Notes on Topical Areas

- Information security / privacy
- Business continuity planning
- Data retention – eDiscovery
- Vendor management / outsourcing
- Financial: remote deposit capture

The Crystal Ball

- The good news – not much brewing!
- Always info security and BCP
- Less controls – could it be?
- Doing more with less
- Resiliency!

Remember…

Awareness

Accountability

Action-ability

Questions / Discussion