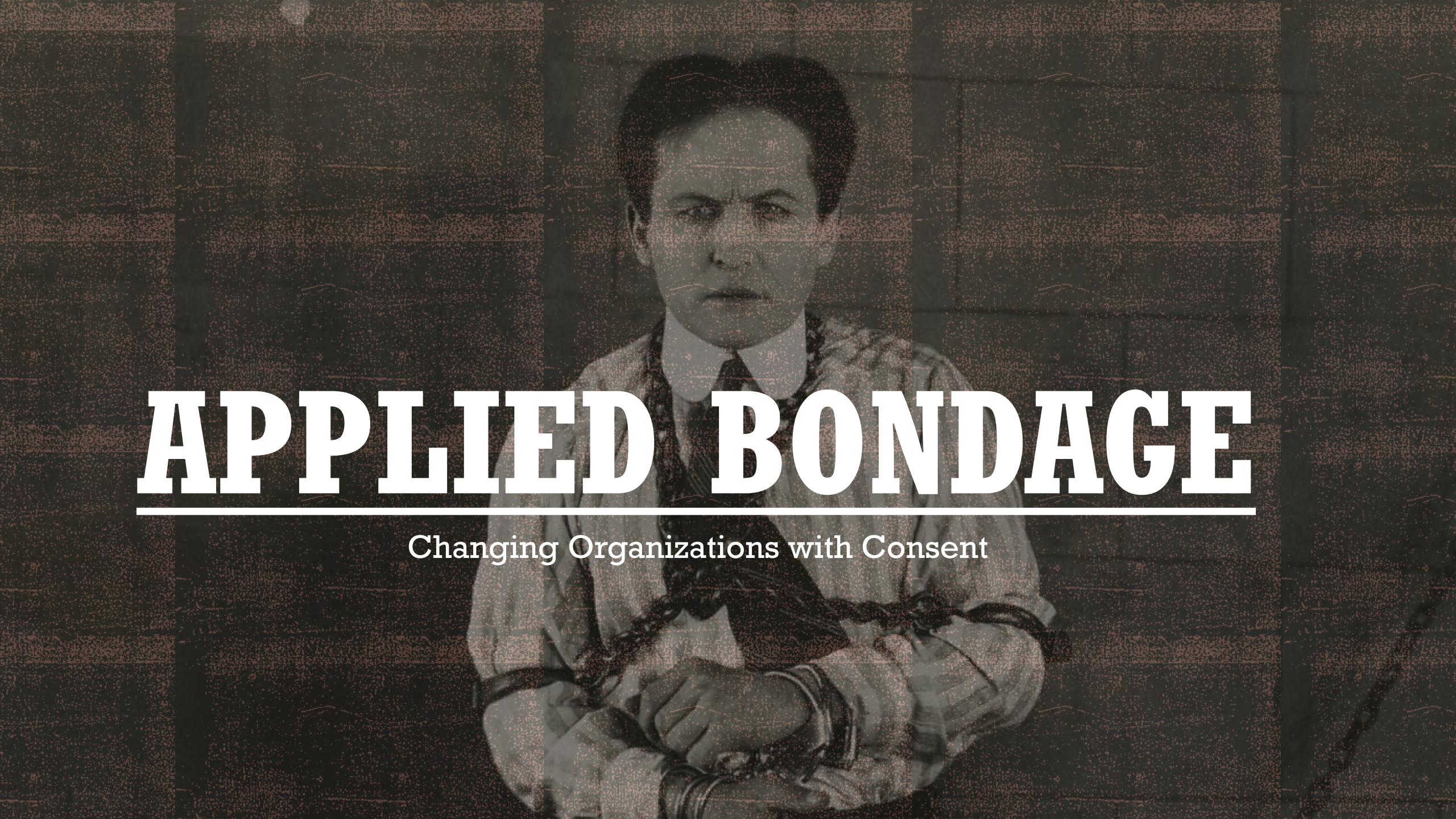


APPLIED BONDAGE

Changing Organizations with Consent

This presentation represents only my own views and not those of my present employer or any past employers.

ANOTHER DISCLAIMER

Je n’ai fait celle-ci plus longue que parce que je n’ai pas eu le loisir de la faire plus courte.*

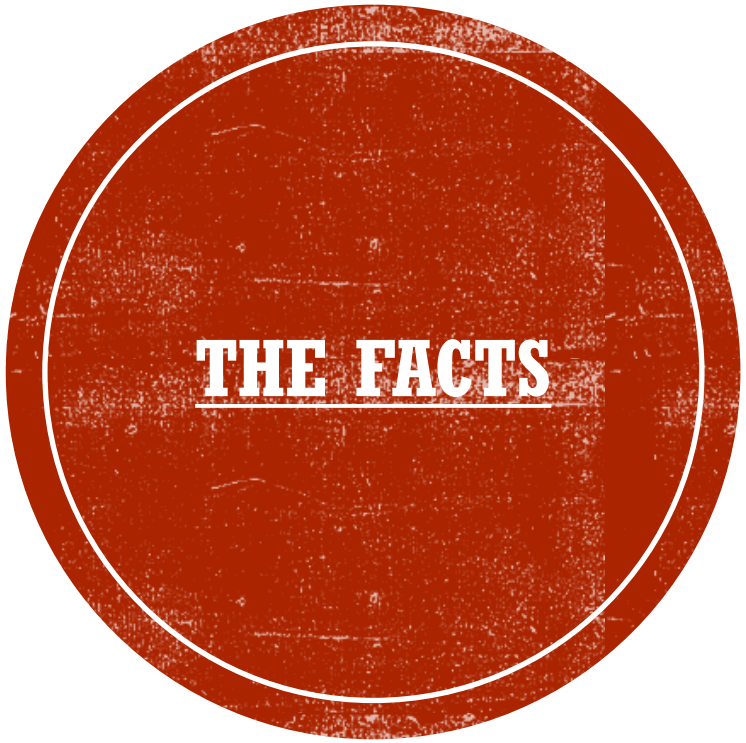
- Blaise pascal

** I have made this longer than usual because I have not had time to make it shorter.*

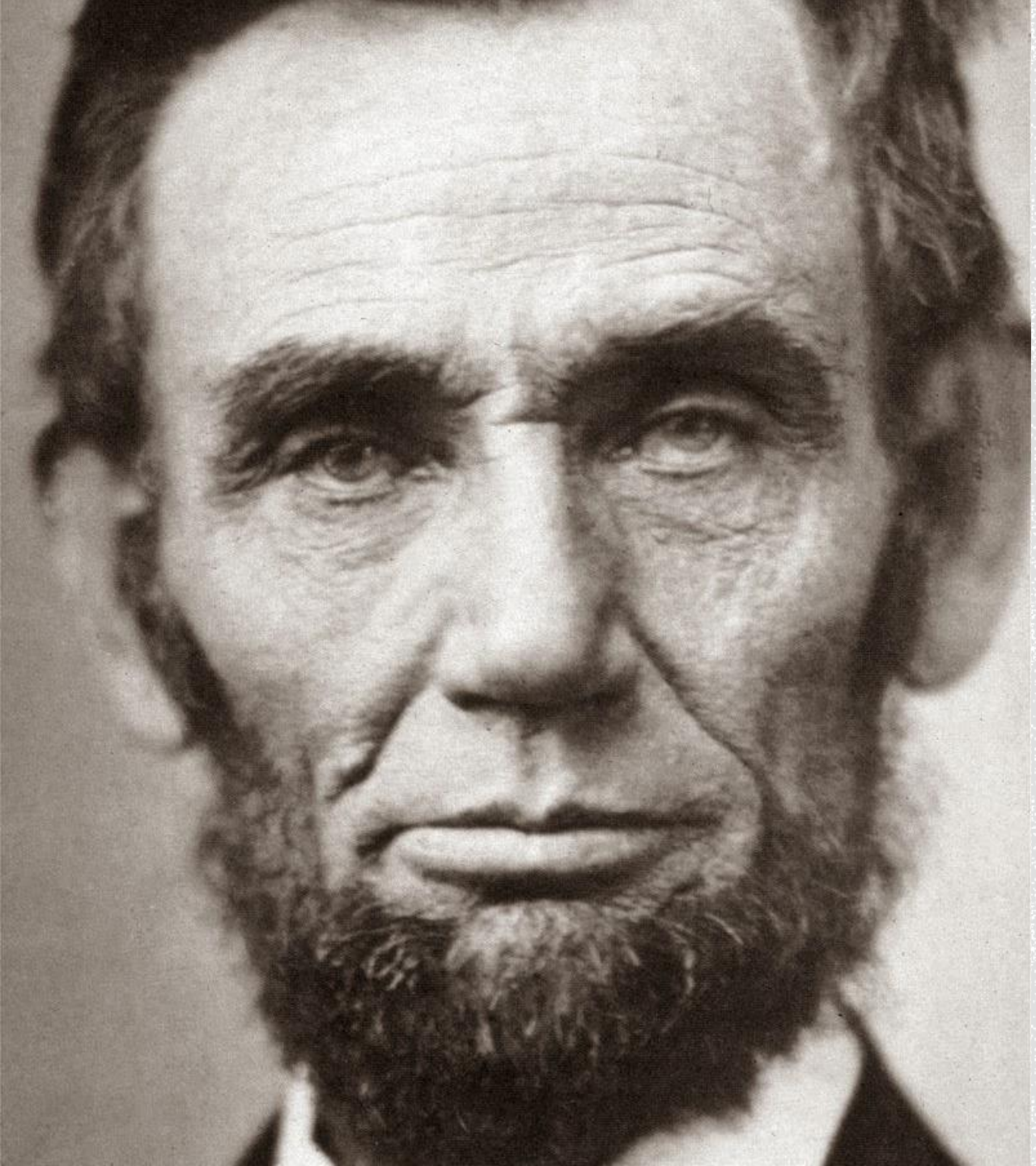
HERMIT

WHO AM I?

- CISO
  - Current: Trinity Rail
  - Former: Westinghouse Nuclear & Celanese
- Acronym holder: RHCSA/RHCE/OSCP/CISSP/etc
- Multiple industries:
  - Dept. of Defense
  - Financial
  - Marketing
  - Manufacturing (chemical/industrial/transportation)
  - Nuclear
- Hacker / CTF & Puzzle enthusiast
- Founder (Cryptolingus, PHA, etc)



- Why do businesses exist?
- What motivates a business to embrace security?
- Who can actually change a business?
- Will you be correct or efficient?



INTEGRITY

- People <u>with</u> integrity will do what they have committed to
- People with integrity like working with similarly aligned people
- People <u>without</u> integrity want to *seem* like they have integrity

- ***NOTE: You must operate with integrity for any of this to work***
- ***NOTE: This approach will not work in a corrupt organization***

TIME CRUNCHES

- This approach is based upon a reasonableness approach
- Time is the primary currency of this approach, and is used to increase pressure

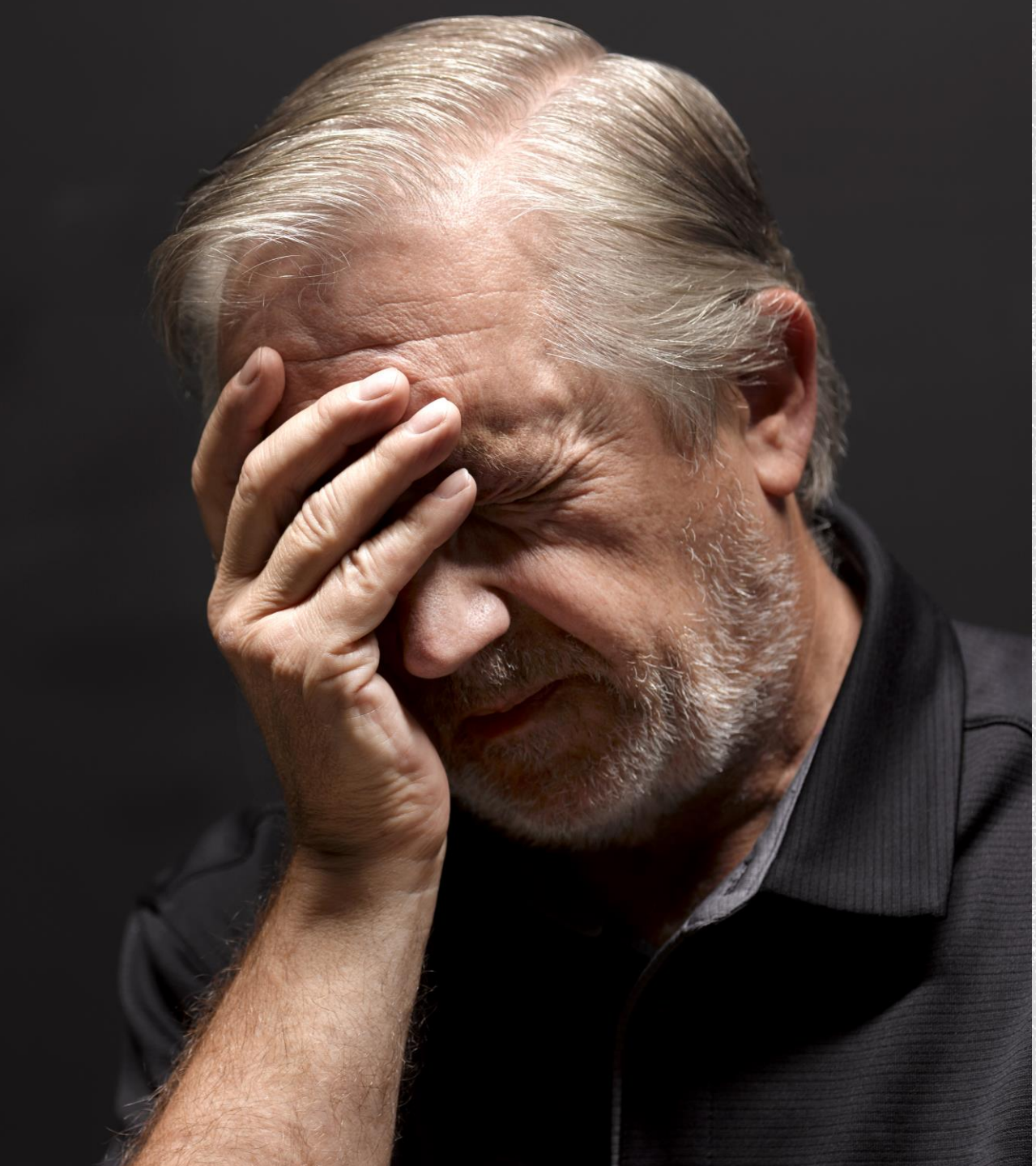
- It's reasonable you haven't cleaned your room today because (reasons)
- It's not reasonable you haven't cleaned your room in two years

COMMON APPROACH

- There are always points where agreement can be found on what should be done
- If you have integrity you want to do what should be done
- No business can always do what should be done

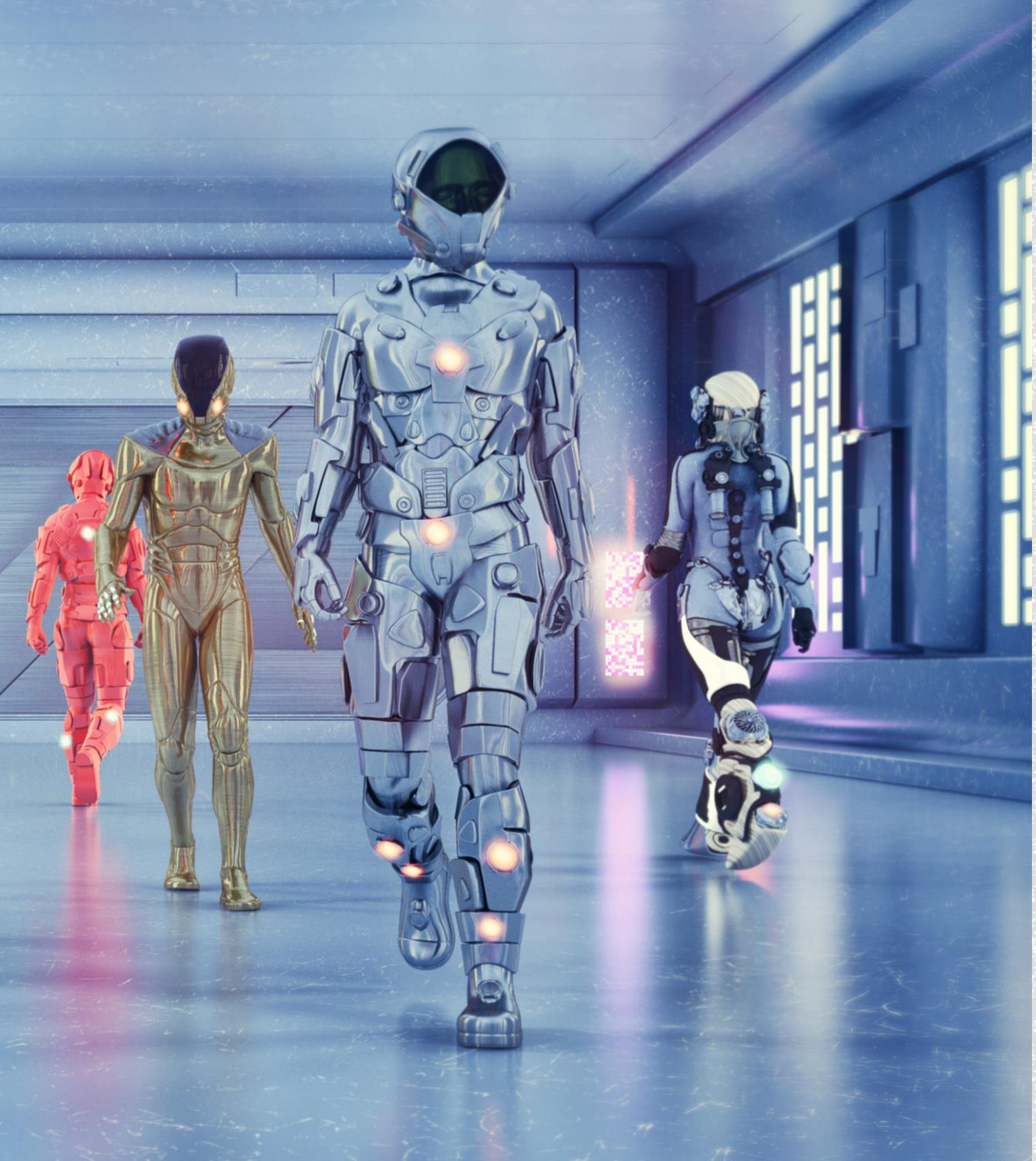
TAKE AWAY THE BLADE

- Defensive postures arise from offensive actions (perceived or real)
- Preventing an offensive action avoids conflict
- People can always hurt themselves !== people can hurt you
- Meet and talk through everything with all stakeholders, don't just publish
- Exceptions should be encouraged
  - Cover for them
  - Visibility for you



PUNISHMENT SUCKS

- People will expose things that will reward them
- People will hide things that will hurt them
- People like being rewarded



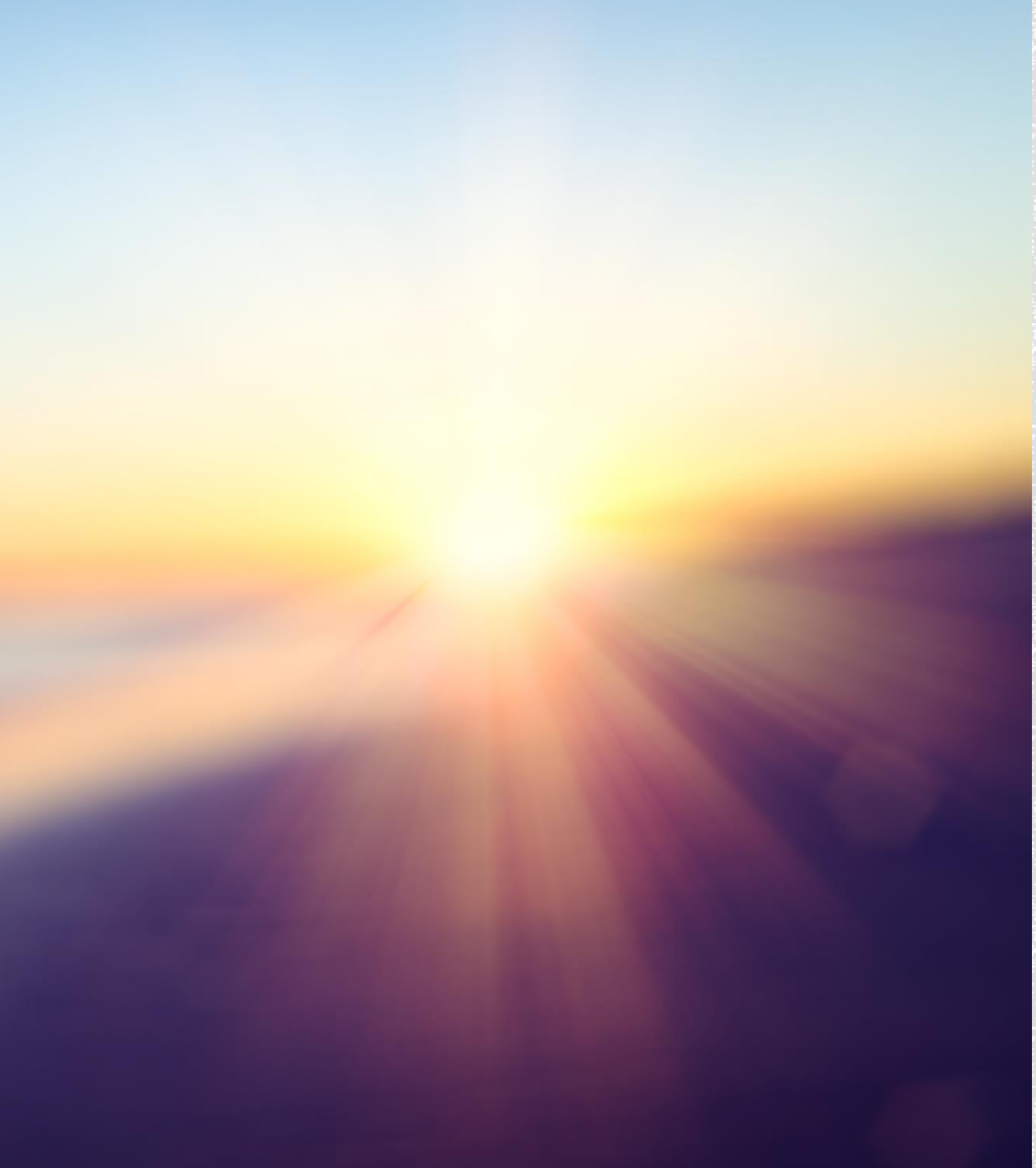
BRUTAL TRANSPARENCY

- You won't change anything if you try to hide the facts
- Practice unavoidable conclusions from common approaches
  - E.g. "we should encrypt all PII" and "we should give people access to their own PII" means "we should encrypt that website providing people access to their PII"
- Communicate methods and approaches before measuring
  - Publish policy, process, standards with grace periods
- Measure and communicate in consistent and automated manners

ACCEPT EXCEPTIONS

- Nothing will be done perfectly
- Consistent exception handling relieves pressure
- Determine who can accept an exception early on
- Exceptions should be:
  - Limited in duration
  - Assessed by a domain expertise
  - Grounded in reality (probability/ likelihood)


THE APPROACH



STEP ONE

Create an Ideal State

Start from nothing. Ignore everything that may currently exist and create an intent that is unencumbered by reality. Assume you have unlimited budget, resources, and executive support.

STEP TWO

Document It

Write down everything you have come up with and make sure it has internal consistency and logic. Each statement should have a known rationale and justification. If it doesn't, remove it.

If you have any existing policies, standards, etc. review them at this time to make sure you have at least equal coverage. If you don't, add and integrate those concepts/intents.

STEP THREE

Build Consensus

Talk to anyone in a leadership, management, or influence role that may be impacted. Talk to everyone you can. Even if you have all the power in the dynamic and they can't stop you from doing something, talk to them.

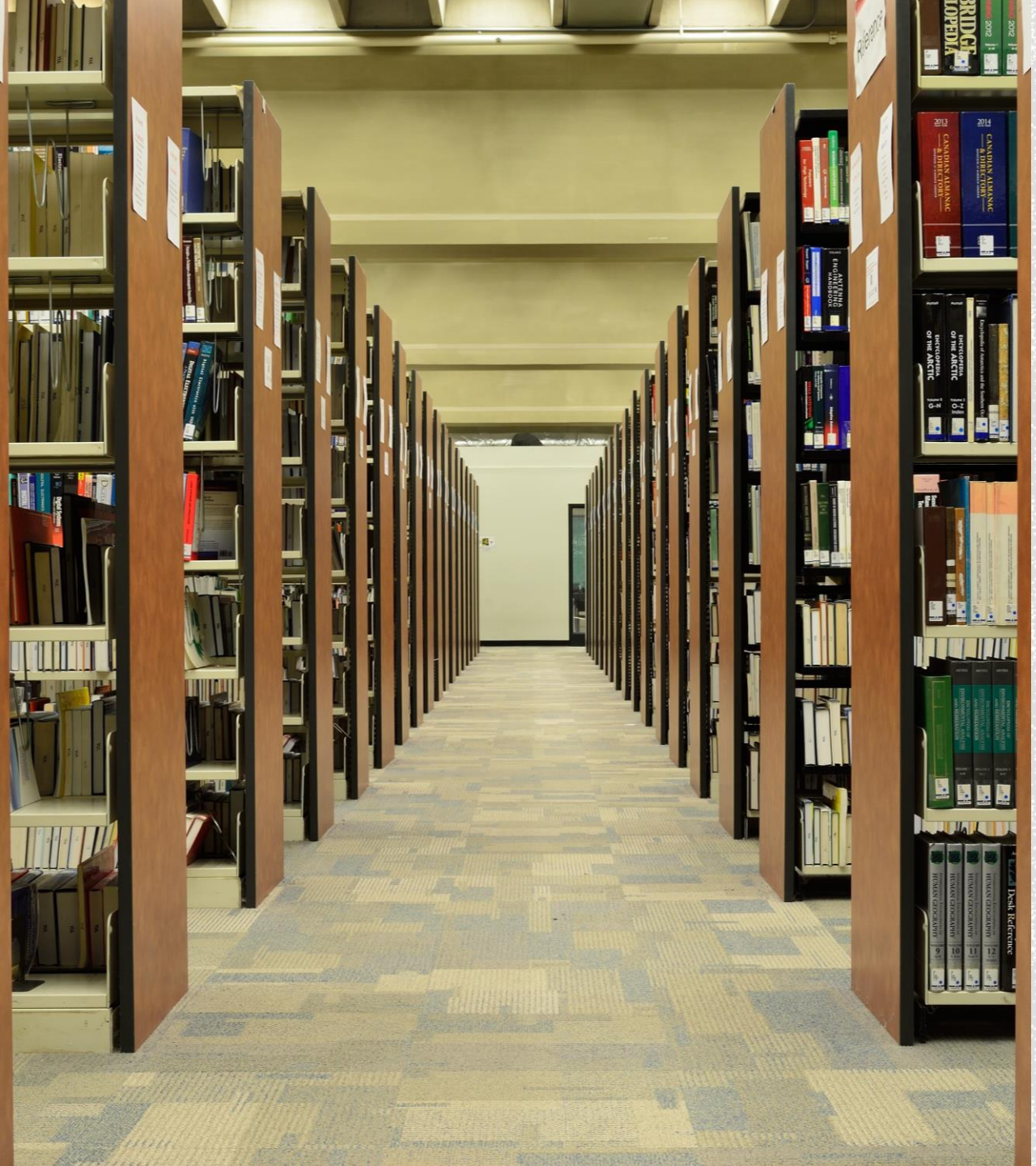
Don't talk at them. Talk to them and listen. Every concern they have should be heard, confirmed as understood, and documented.

STEP FOUR

Make Concessions (Take Away the Blade)

Reconcile as many of the concerns as you can, and update to address them. Concessions are your friend. Concessions allow each party to take ownership of and invest in the outcome. Make them freely.

It's a lot harder to attack a document/policy/approach that you helped author.



STEP FIVE

Make it Accessible

Translate the document (if required), get approvals, and put it somewhere that is version controlled, tracked, searchable, and discoverable. Make it a common point of reference that anyone and everyone can see and use.

And if that doesn't exist, build it by following this same approach.

STEP SIX

Make it Known

Tell everyone that something new exists. Tell them what it means to them. Tell them where to find it. But most importantly, host sessions to discuss any concerns that people may have.

Be open, accessible, and brutally transparent. If something will be painful, own it, but identify the rationale and process that built consensus to get to this point.

STEP SEVEN

Give Time to Align

Nothing can be aligned and fixed in a short period of time. Change requires time to plan, understand impacts, seek exceptions, communicate intent, implement, and review.

Give people time between when a document is published and when it comes into effect. Give them twice as long as you think is reasonable to accomplish the asks. Consider what other priorities exist.

STEP EIGHT

Make it Measurable

Establish what the critical aspects are, how they can be measured, what dimensions (e.g. risk, cost, % completion) are informative, and how that data can be captured and evaluated across multiple dimensions (organization, business unit, location, management, etc).

Communicate this information to everyone involved and make concessions on the approach.

STEP NINE

Make it a Priority

Most companies have safety and compliance metrics built into the performance goals of leadership and management. Add performance goals aligned to the measurements for everyone who can influence the outcome.

Remember, exceptions exist and can and should be used. If a team/group can't hit a target document what is reasonable, then work to improve that next cycle.

STEP TEN

Make it Fair

Measure using the approaches agreed upon. Measure every involved stakeholder. Don't hide or justify. If you are the cause of a bad measurement, own it.

Make the measurements consistently and (ideally) automatically.

Focus on short and long term trends, not points in time.

VICTORY

Continue the process. Let each participant approach this however they would like.

Lots of exceptions? Sure thing, as long as there is appropriate approval.

Over time those who align and establish efficient ways of meeting the intents will naturally be identified, and excuses/avoidances/etc. will naturally be corrected or removed.

Dirty rooms can only stay dirty for so long.

THE RESULT

- Stakeholders have input into their assessment
- Stakeholders have agency in performance measurement
- Excuses are eroded and destroyed by time and facts
- Bad things will remain… and that's okay (for now)
- Good things get visibility and reinforcement
- Feuds and bad blood are avoided

Sprinkles? Heck yeah, sprinkles. Winners get sprinkles.