RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **RMG-W08**

Risk Management: Hindsight is 2020

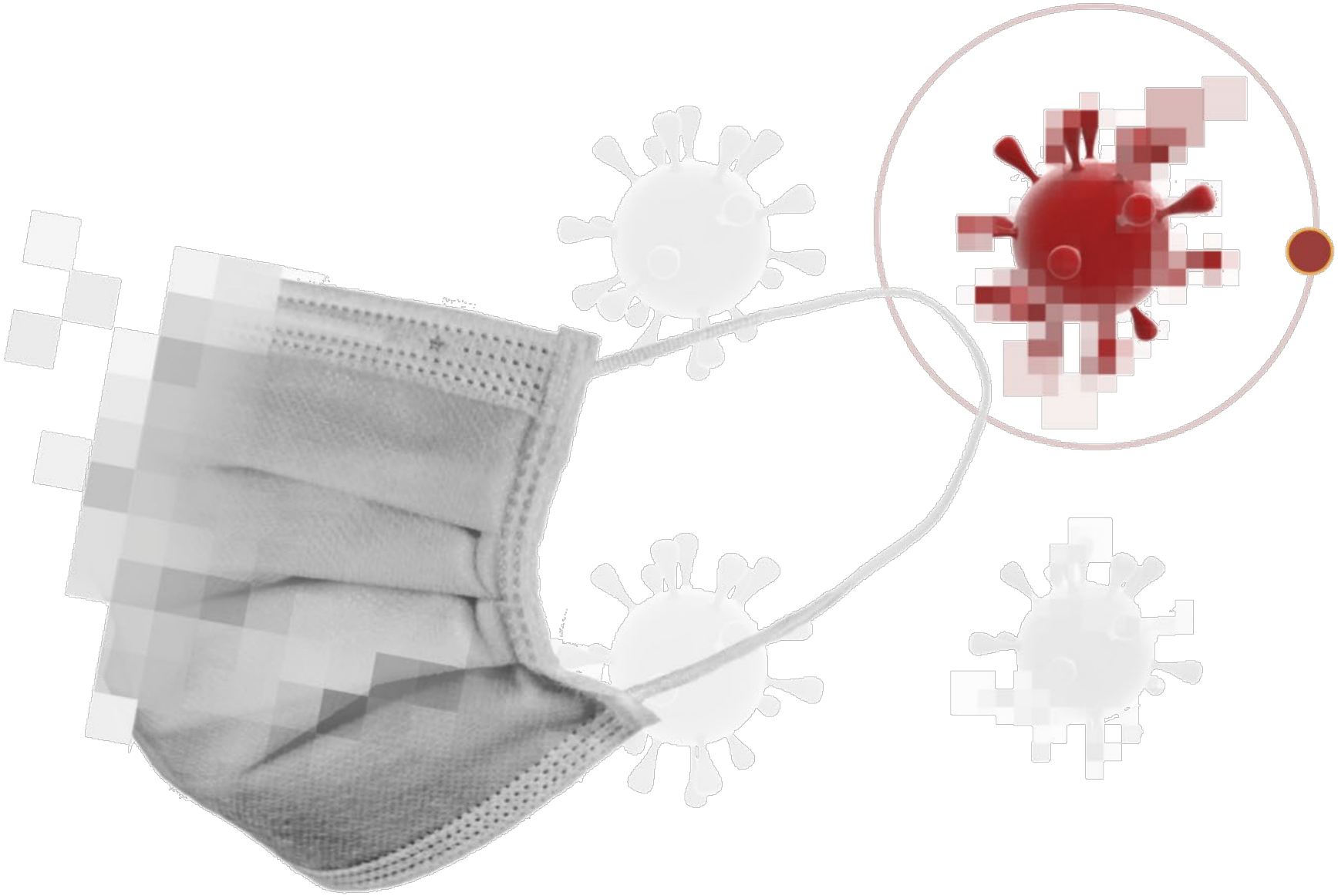
J Wolfgang Goerlich

Duo Advisory CISO
Cisco Secure
@jwgoerlich

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.



Hindsight is 2020

In Scope

- NIST Risk Management Framework.
- Psychology and the pandemic.
- Suggestions on how to improve risk management.

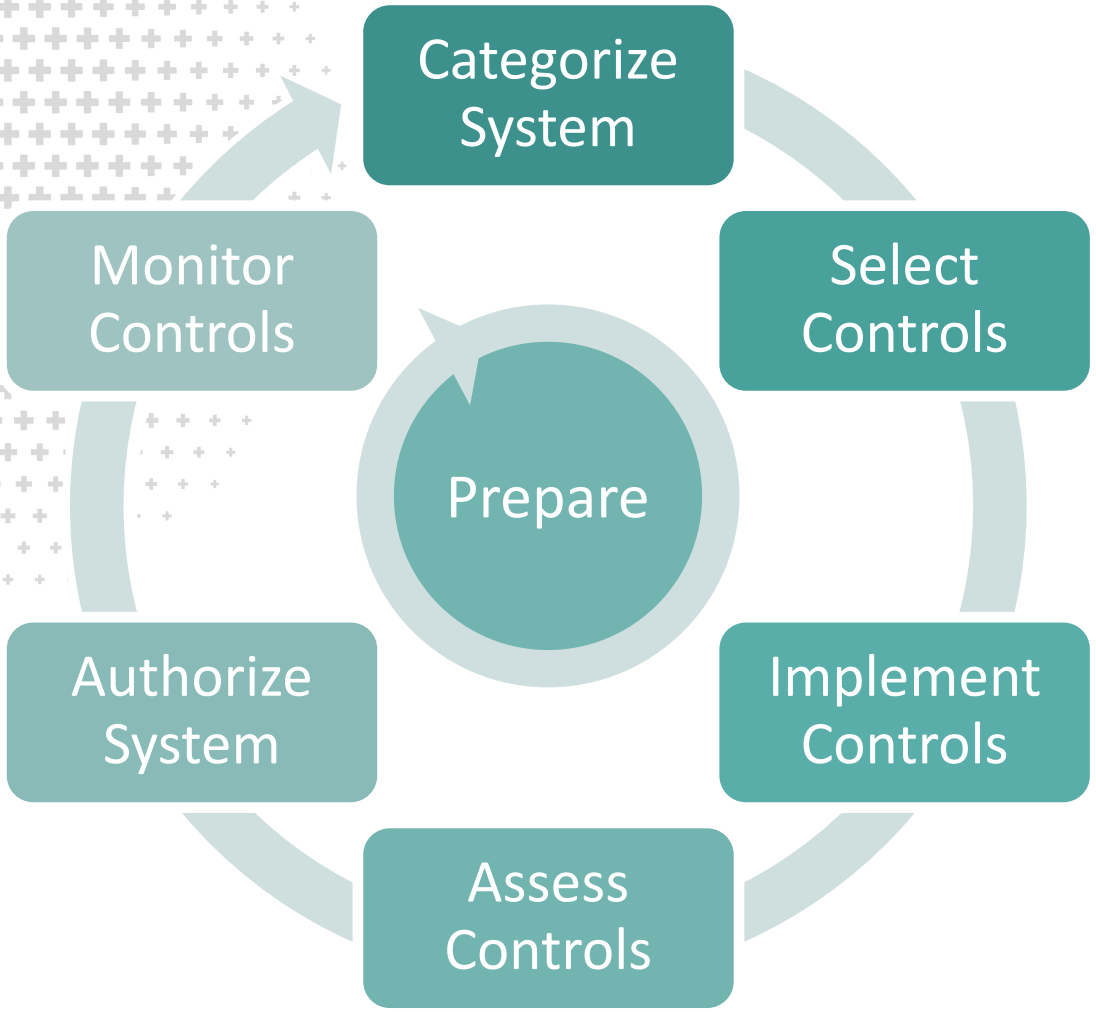
Out of Scope

- This is not a replacement of risk management fundamentals.
- This is not a search for a silver lining in the pandemic.
- This is not a medical science talk. I will make simplifications during this talk.

The Human Condition is One of Ignoring Risk.

(Risk Management as Taught)

(Risk Management as Practiced)



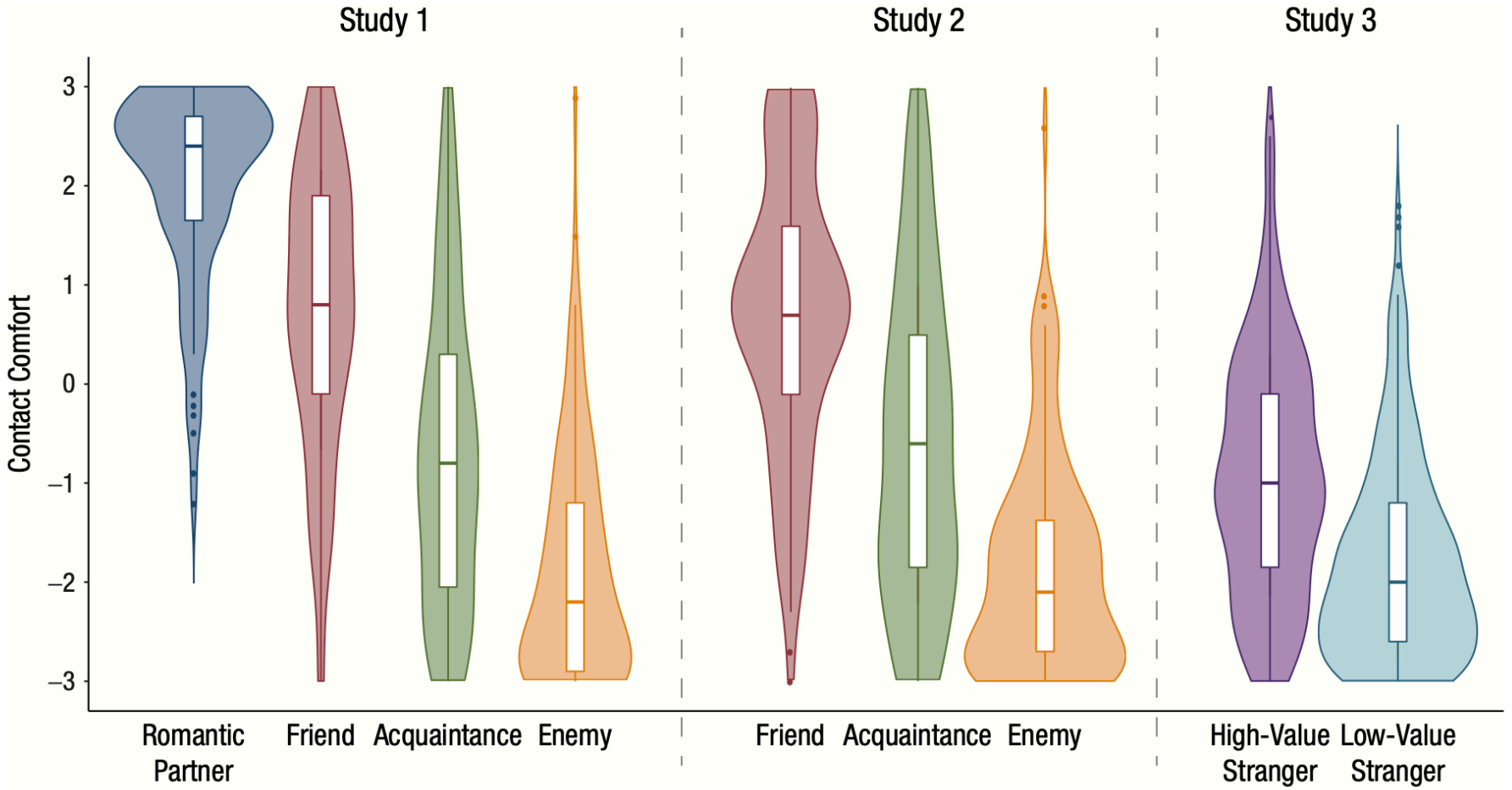
Prepare

- Roles and responsibilities
- Strategy and risk tolerance
- Organizational risk assessment
- Control baseline & framework
- Impact level
- Continuous monitoring

The Human Experience of Risk

- Risk tolerance varies by the person asking or person deciding
- Perception of risk influenced by salience and availability biases
- Decision-making prefers certainty while risk delivers uncertainty
- Relationships, trust, personal experiences outperform statistics

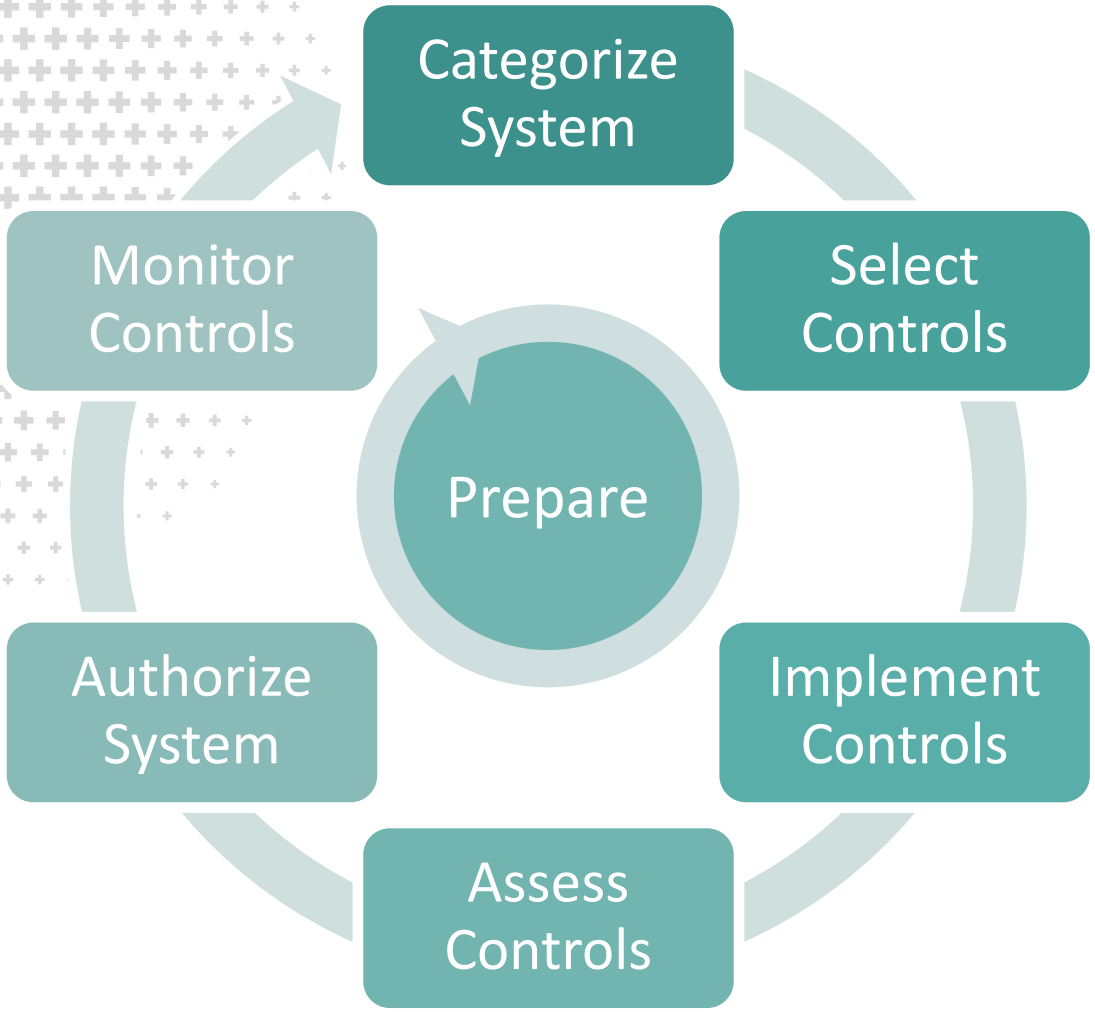
Who's Asking?



Source: Tybur, Joshua M; Lieberman, Debra; Fan, Lei; Kupfer, Tom R; de Vries, Reinout E. "Behavioral Immune Trade-Offs: Interpersonal Value Relaxes Social Pathogen Avoidance"

Preparation Tips

- Build relationships and build trust ***before*** presenting data
- Communicate salient risk scenarios ***with*** data
- Make the important interesting, make the interesting important



Categorize

- System description
- Security categorization
- Review and approval

The Human Experience of Risk

- We teach risk as a function of quantifiable measures
  - { (confidentiality, impact), (integrity, impact), (availability, impact) }
- People experience risk qualitatively, driven by perception
  - (hazard, outrage)
- Decisions like categorization are not black-and-white

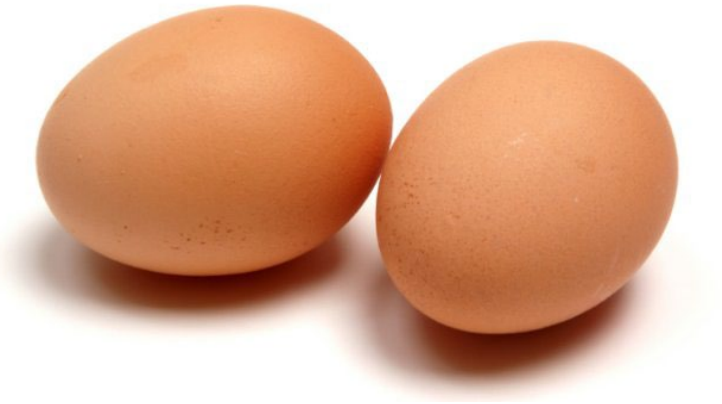
Source: Peter Sandman, *Responding to Community Outrage: Strategies for Effective Risk Communication*

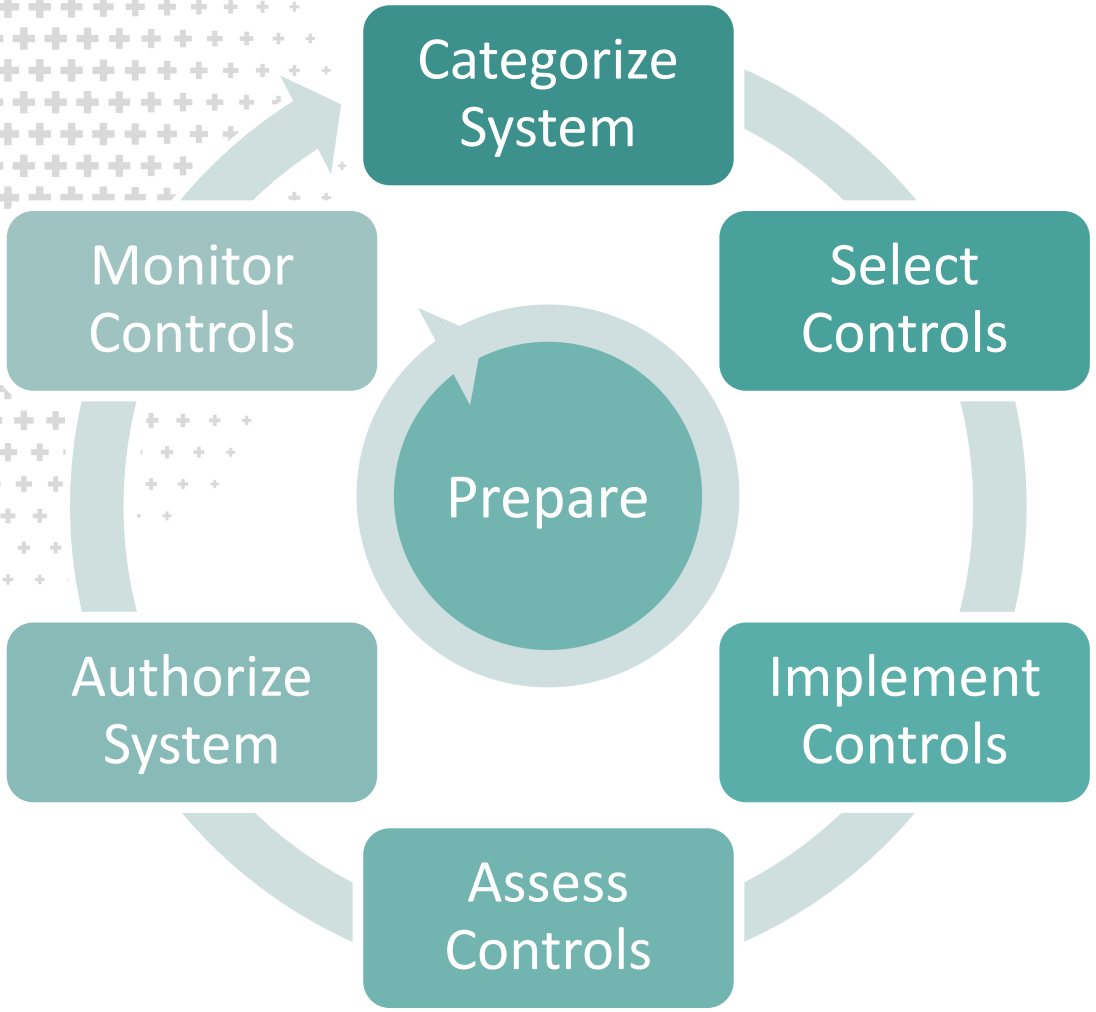
What's The Worse That Could Happen?

Source: Barasz, Kate; Hagerty, Serena F. "Hoping for the Worst? A Paradoxical Preference for Bad News"

Categorize Tips

- Reflect internal and external perception in risk scoring
- Simplify the decisions to avoid paralysis (red, yellow, green)
- Prebunk any potential misinformation





Select Controls

- Select, tailoring, allocation
- Implementation plan
- Continuous monitoring plan
- Review and approval


AT LEAST
6 FEET


COVID-19


KN95
GB2626-2019


Vaccine
COVID-19

But in Our Case …

- Identification, Authentication, Access Control
- Business Continuity and Disaster Recovery
- Configuration Management
- Secure Software Development Lifecycle
- Security Awareness and Training
- System and Services Acquisition

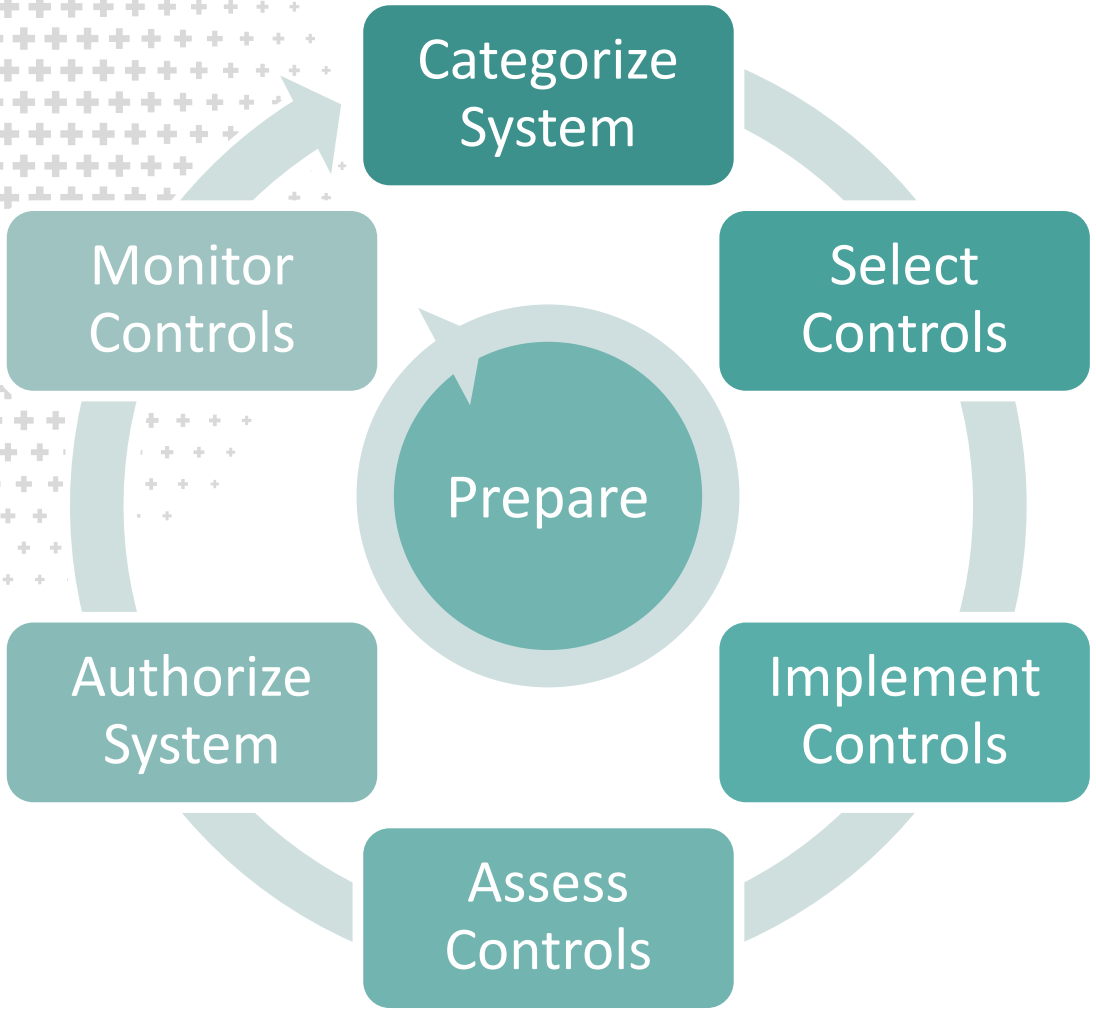
The Human Experience of Risk

- Controls meet individual pushback -- psychological resistance
- Personally, people have a risk thermostat
- Collectively, organizational cultures have a risk equilibrium

Risk Thermostat

Controls Tips

- Premortem on the implementation and monitoring plans
- Plan changes in our processes and technology
- Communicated in a language the audience understands
- Increasing the understanding of the risk scenario and how the selected controls will address the risk
- Monitor to not incur new risks due from secondary behaviors

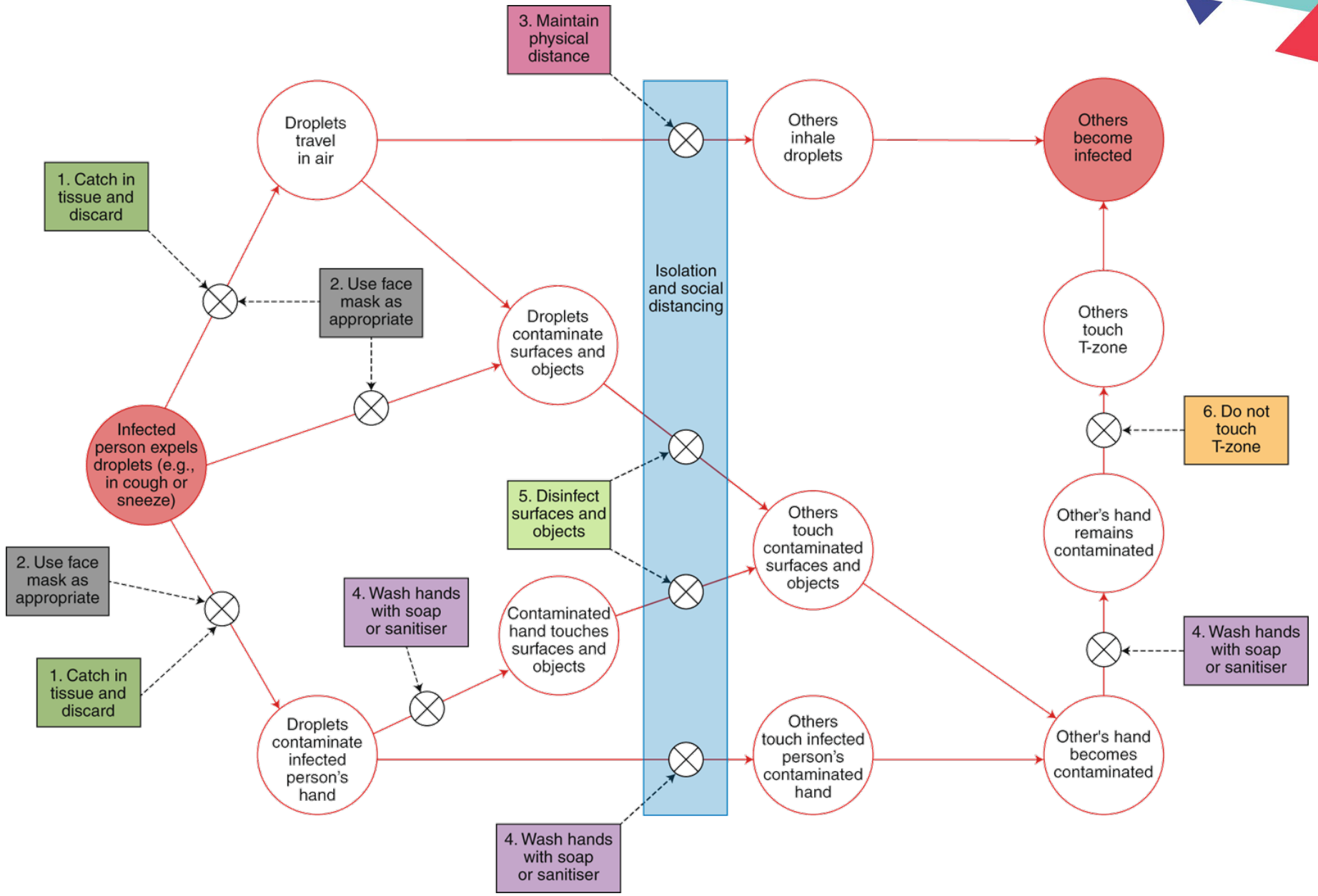


Implement

- Control implementation
- Documentation

The Human Experience of Risk

- Risk habituation fuels resistance to change
- Facts don’t change minds, stories do
- People have a finite capacity for absorbing new changes
- People have a limited ability to focus on changing (50-150 days)
- Awareness training can’t overcome barriers

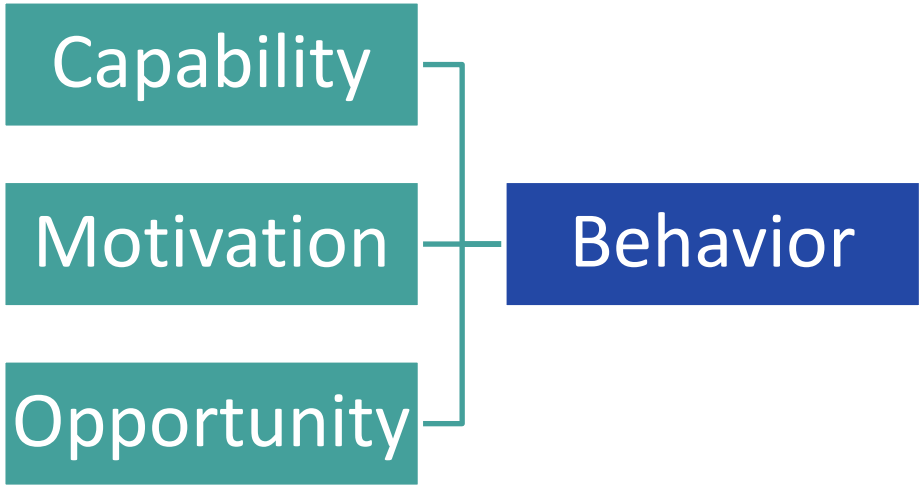


Source: West, Robert; Michie, Susan; Rubin, G James; Amlôt, Richard. Applying principles of behaviour change to reduce SARS-CoV-2 transmission.

Adherence – COM-B Model

- Test and trace broke down in the UK because of inability to recognize Covid symptoms and financial hardship

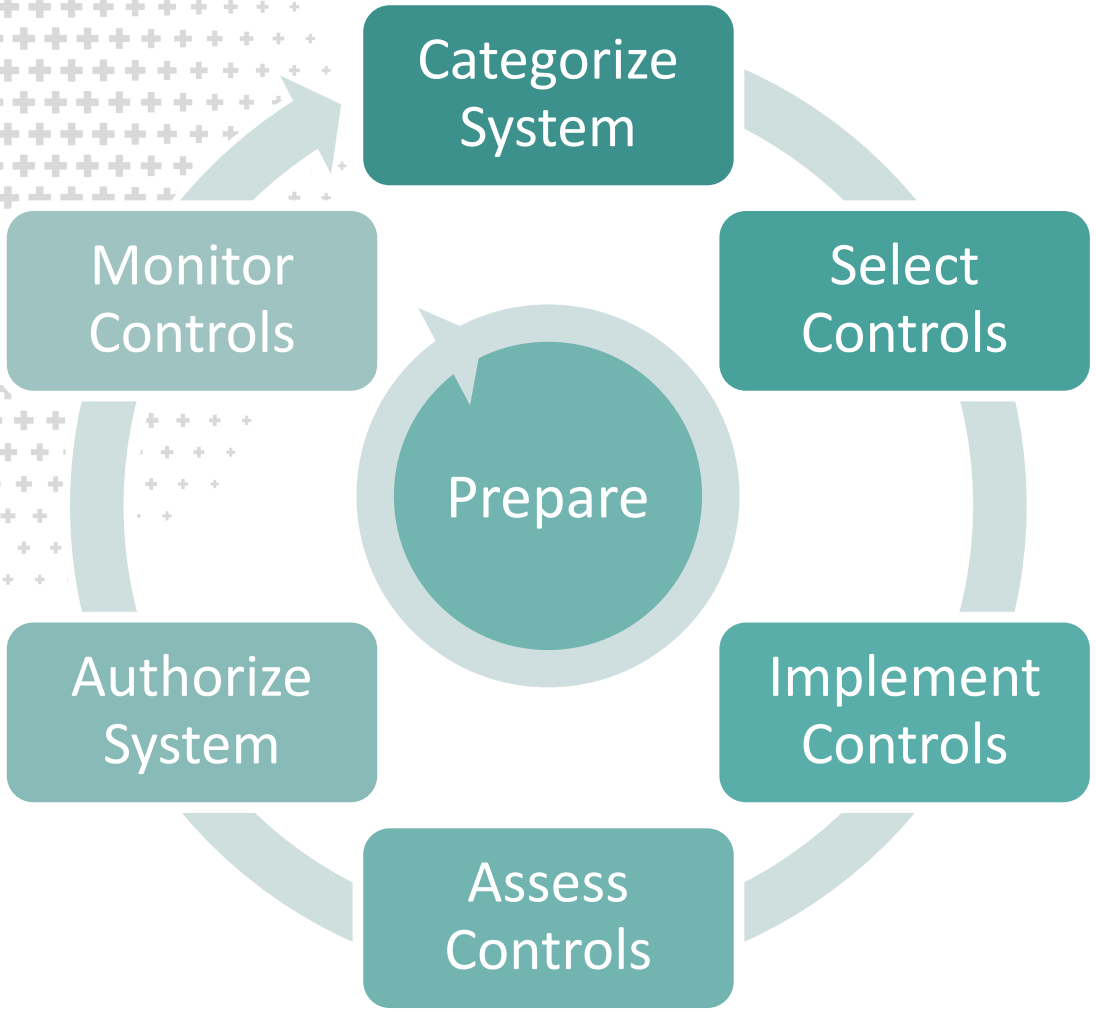
- Implementation should focus on:
  - Capability – can they do it?
  - Motivation – do they want to do it?
  - Opportunity – what's blocking them?



Source: Smith, Louise E; Potts, Henry W W; Amlôt, Richard; Fear, Nicola T; Michie, Susan; Rubin, G James. Adherence to the test, trace and isolate system: results from a time series of 21 nationally representative surveys in the UK.

Implementation Tips

- Leverage the fresh start effect – new system, new year
- Design controls with behavior changes
- Make it personal, make it specific, make it familiar
- Match implementation to the organization's capacity to change
- Postmortem the implementation, debunk misinformation



Assess Controls

- Team selection
- Assessment plan
- Control assessment
- Assessment report
- Remediation
- Plan of Action & Milestones (POA&M)

The Human Experience of Risk

- What we intend isn't what we do; intention-behavior gap
- What we say isn't what we do; description-experience gap
- What we do isn't consistent

Embed Security Practices into Lifecycle Events

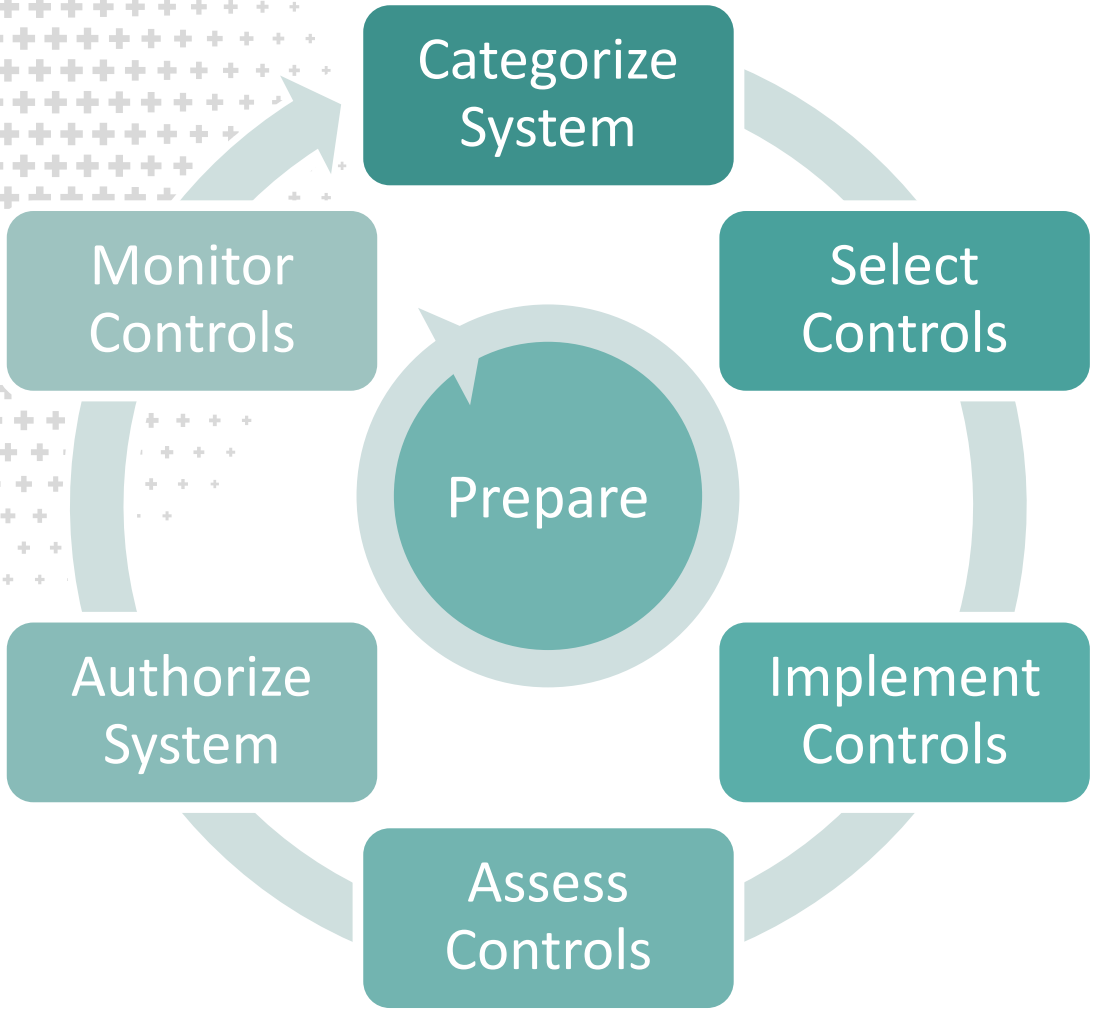
Think Things → Plan a Thing → Do a Thing → One More Thing → Check the Thing → Finish the Thing

Source: Aunger, Robert; Schmidt, Wolf-Peter; Ranpura, Ashish; Coombes, Yolande; Maina, et al; Three kinds of psychological determinants for hand-washing behaviour.

Assessment Tips

- Embed security controls and practices into lifecycle events
- Control validation: existence, effective, operationalized
- Exceptions and audit findings are feedback on implementation

People breaking the rules are people communicating to us our design problems.



Authorize System

- Authorization Package
- Risk analysis
- Risk response
- Authorization decision
- Reporting

The Human Experience of Risk

- Risk tolerance changes from then to now; risk habituation
- Relationships, trust, personal experiences shift perspective
- A minority of loud naysayers outweigh a majority of supporters


BIBERTO
MEDIUM

When Work Looks Like Work, Work Gets Done.

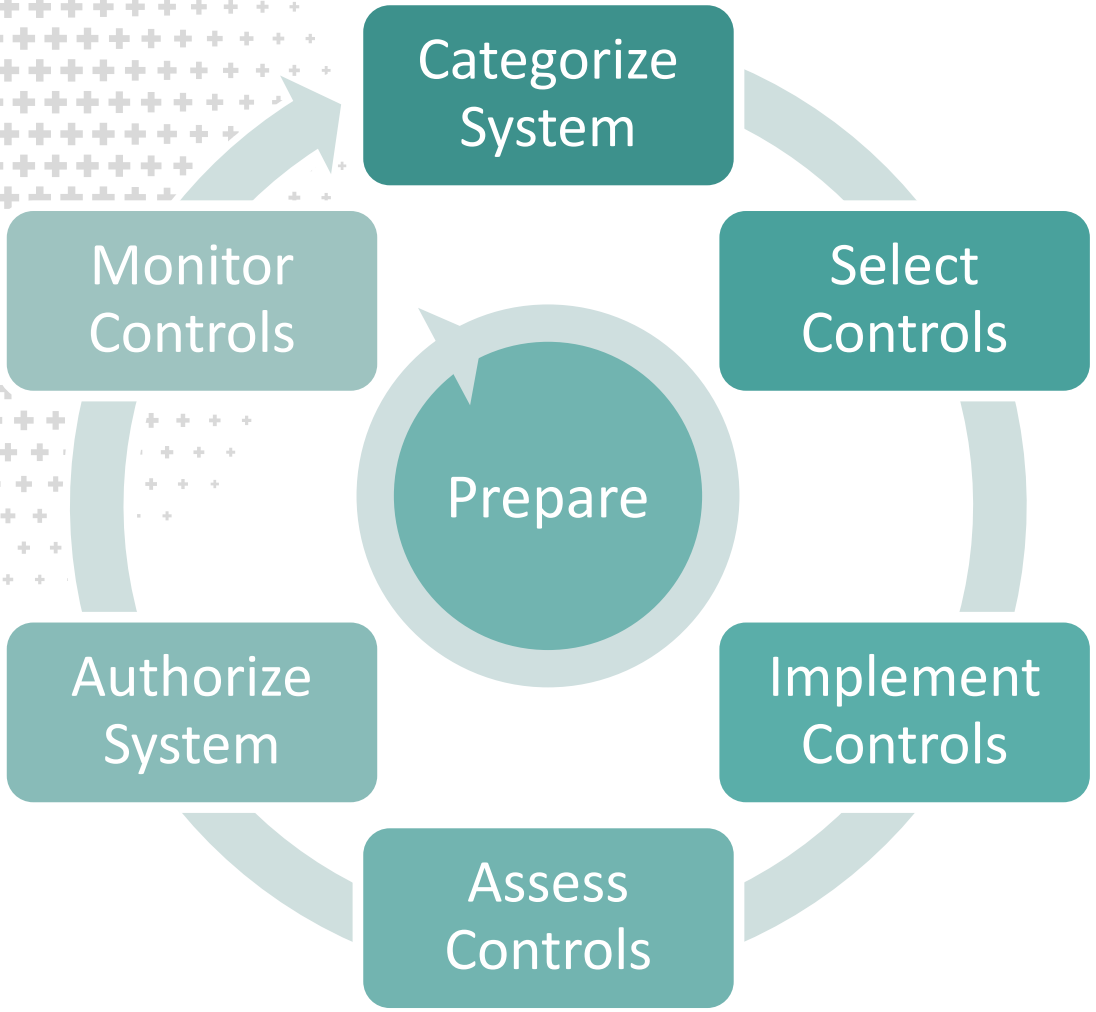
- Messaging which looks like we expect is more effective messaging

- Use the same risk reporting presentation
- Use the same spreadsheets
- Use the same after-action process
- Use KPI or OKR or whatever the business uses

Source: Milkman, Katherine L; Patel, Mitesh S; Gandhi, Linnea; et al. A megastudy of text-based nudges encouraging patients to get vaccinated at an upcoming doctor's appointment

Authorization Tips

- Define authorization decision criteria early and clearly
- Questioning the data is feedback on the relationship
- Consistent communication over an extended term
- Leverage familiar communication language, style, cadence



Monitor Controls

- Change management
- Ongoing assessments
- Ongoing risk response
- Authorization package updates
- Security and privacy reporting
- Ongoing authorization

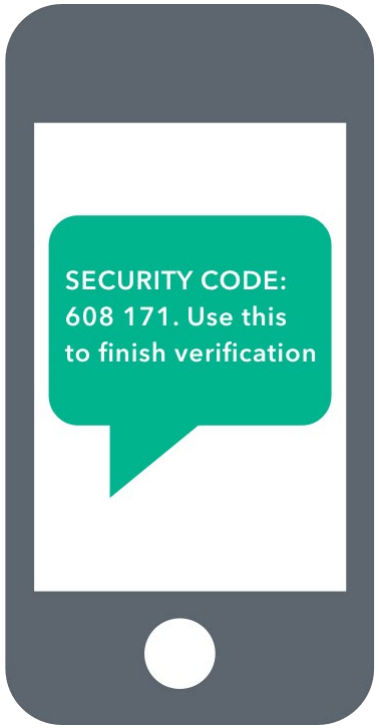

PANIC

The Human Experience of Risk

- Operational issues reduce trust in the controls
- Controls are in place, however, bad things happen anyway
- Controls are in place, however, effectiveness reduces over time

Time it takes to transmit an infectious dose of Covid-19

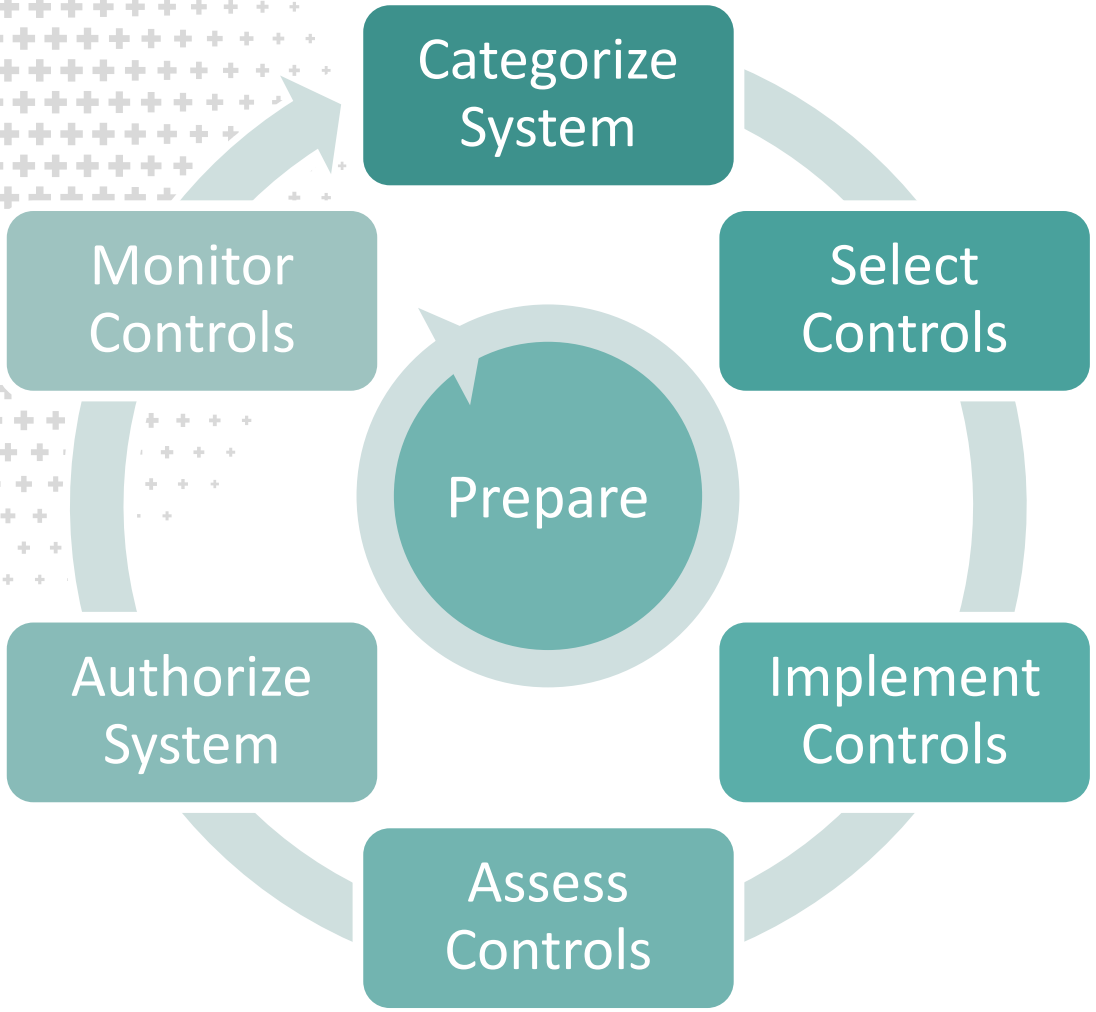
PERSON INFECTED IS WEARING	PERSON NOT INFECTED IS WEARING: Nothing	Cloth mask	Surgical mask	N95
Nothing	15 min.	20 min.	30 min.	2.5 hours
Cloth mask	20 min.	27 min.	40 min.	3.3 hours
Surgical mask	30 min.	40 min.	1 hour	5 hours
N95	2.5 hours	3.3 hours	5 hours	25 hours



Source: WSJ, "Why Cloth Masks Might Not Be Enough as Omicron Spreads" https://www.wsj.com/articles/cloth-face-mask-omicron-11640984082

Monitoring Tips

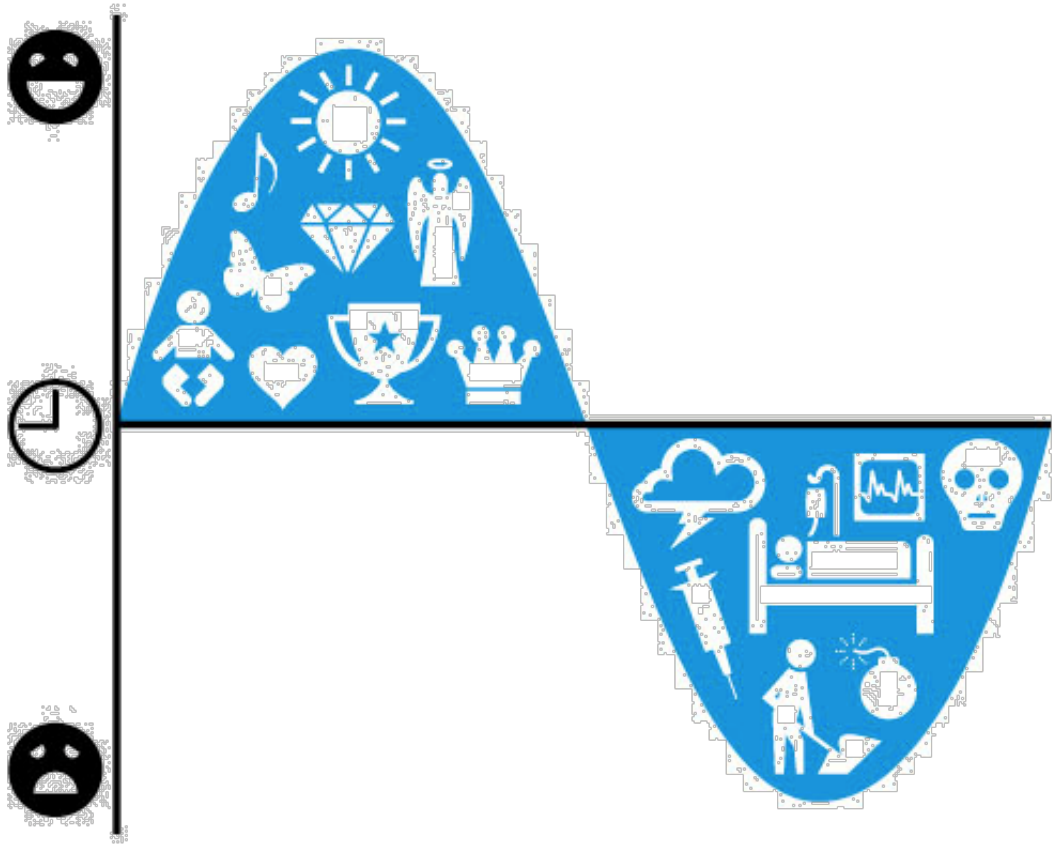
- Communicate salient risk scenarios ***with*** evolving data points
- Find unexpected benefits and amplify those benefits
- Address unexpected barriers



Prepare

- Roles and responsibilities
- Strategy and risk tolerance
- Organizational risk assessment
- Control baseline & framework
- Impact level
- Continuous monitoring

Space Shuttle Challenger and Memory



Sources: Kurt Vonnegut, On The Shape Of A Stories
Andrew J Reagan1; et al. The emotional arcs of stories are dominated by six basic shapes

Risk is **not** the language of business.
Story is.

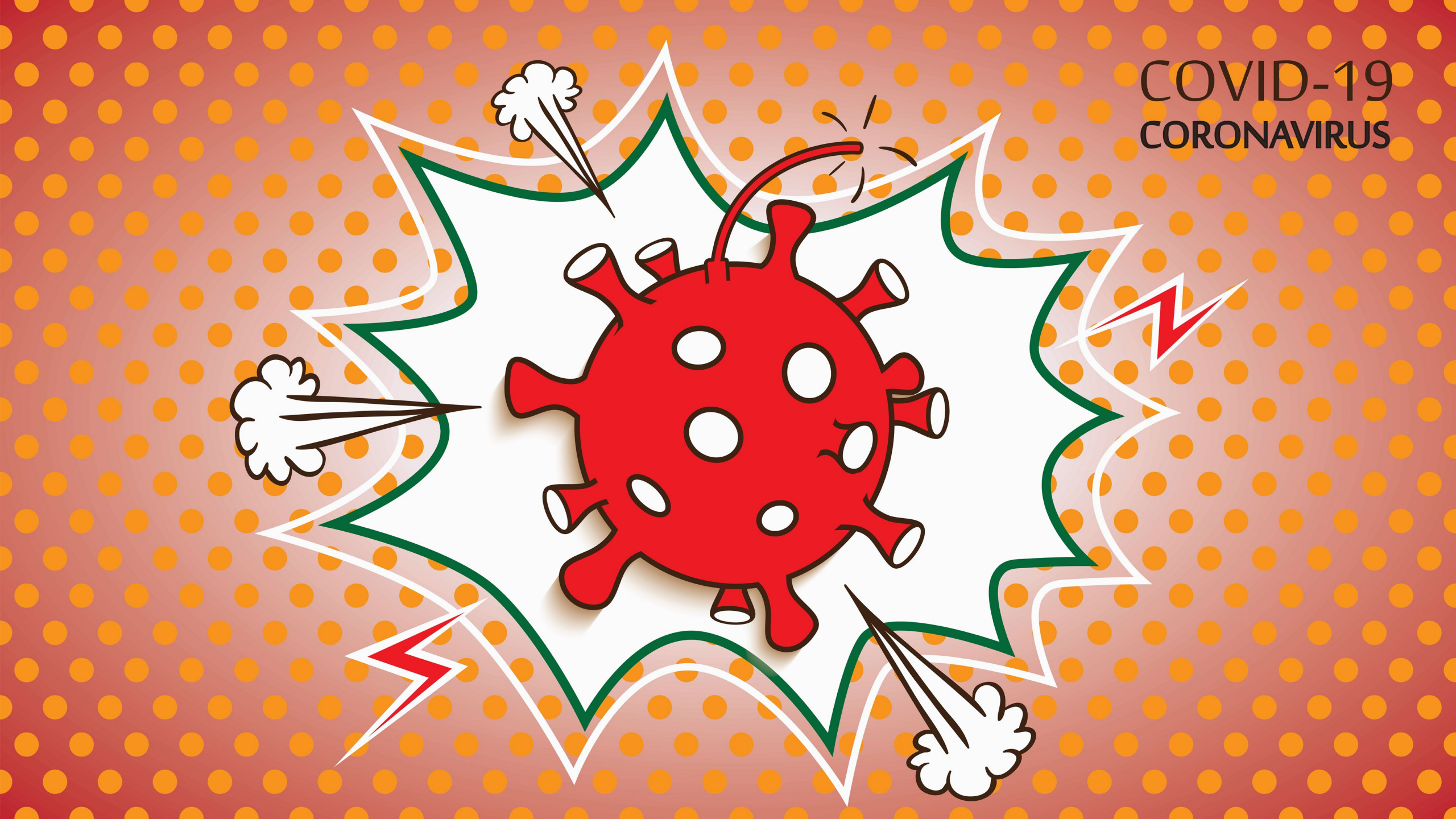
More Preparation Tips

- Manage the story – Shape of Story
- Manage the relationships – The Infinite Game
- Manage the risk appetite and tolerance – psychological resistance, risk thermostat, risk habituation

We prepare for tomorrow's risk management cycle with the work we perform during today's risk management cycle.

RSAConference2022

Final Thoughts


COVID-19
CORONAVIRUS

Recap

- We have a good idea of what our workforce needs to be secure. We have some behaviors they need to follow. Yet time and again, our approaches fail.
- The pandemic provided a unique opportunity to see how this problem plays out in other fields.
- Draw lessons for security while the pandemic is still a fresh and shared experience.

Cottage Core

Goblin Mode

Practical Steps towards Human-centered Risk Management

- Next week you should:
  - Identify areas of the risk management program that have stalled or failed to gain support
  - Workshop these areas looking for salience, habituation, resistance, misinformation
  - Perform a stakeholder analysis and find any low trust relationships
- In the first three months following this presentation you should:
  - Adjust conversation on risk to better align with the psychology of risk
  - Put in place a cadence with low trust stakeholders – manage the relationships
  - Change from risk appetite to a risk menu – specific scenarios supported by data
  - Shift risk treatment and control implementation to focus on lifecycle events
- Within six months you should:
  - Change reporting on risk treatment to emphasize story over statistics – manage the story
  - Evaluate risk assessment and treatment results, collect lessons learned
  - Expand the approach into other areas of the risk management program

Thank you!

cisco SECURE