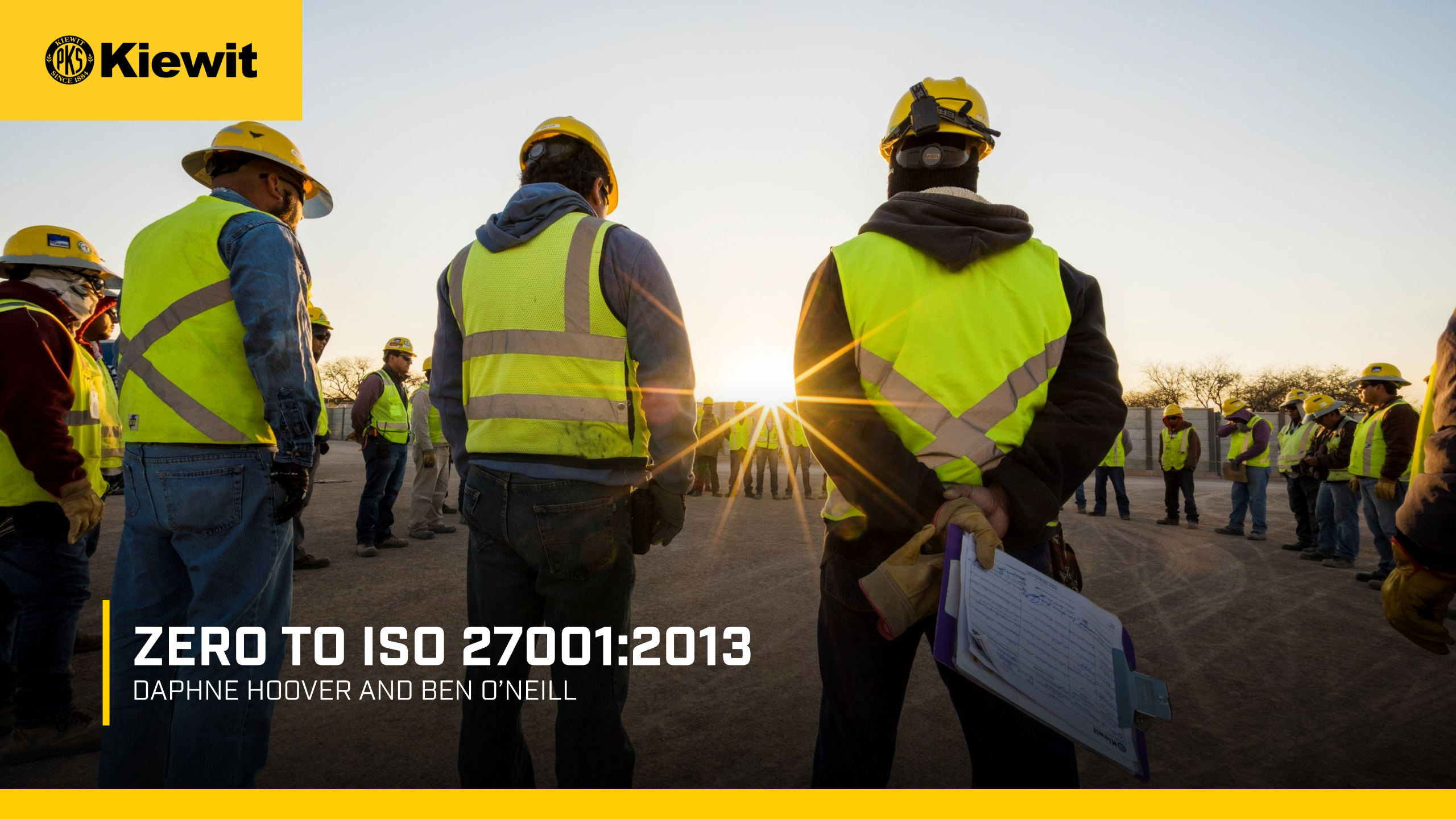
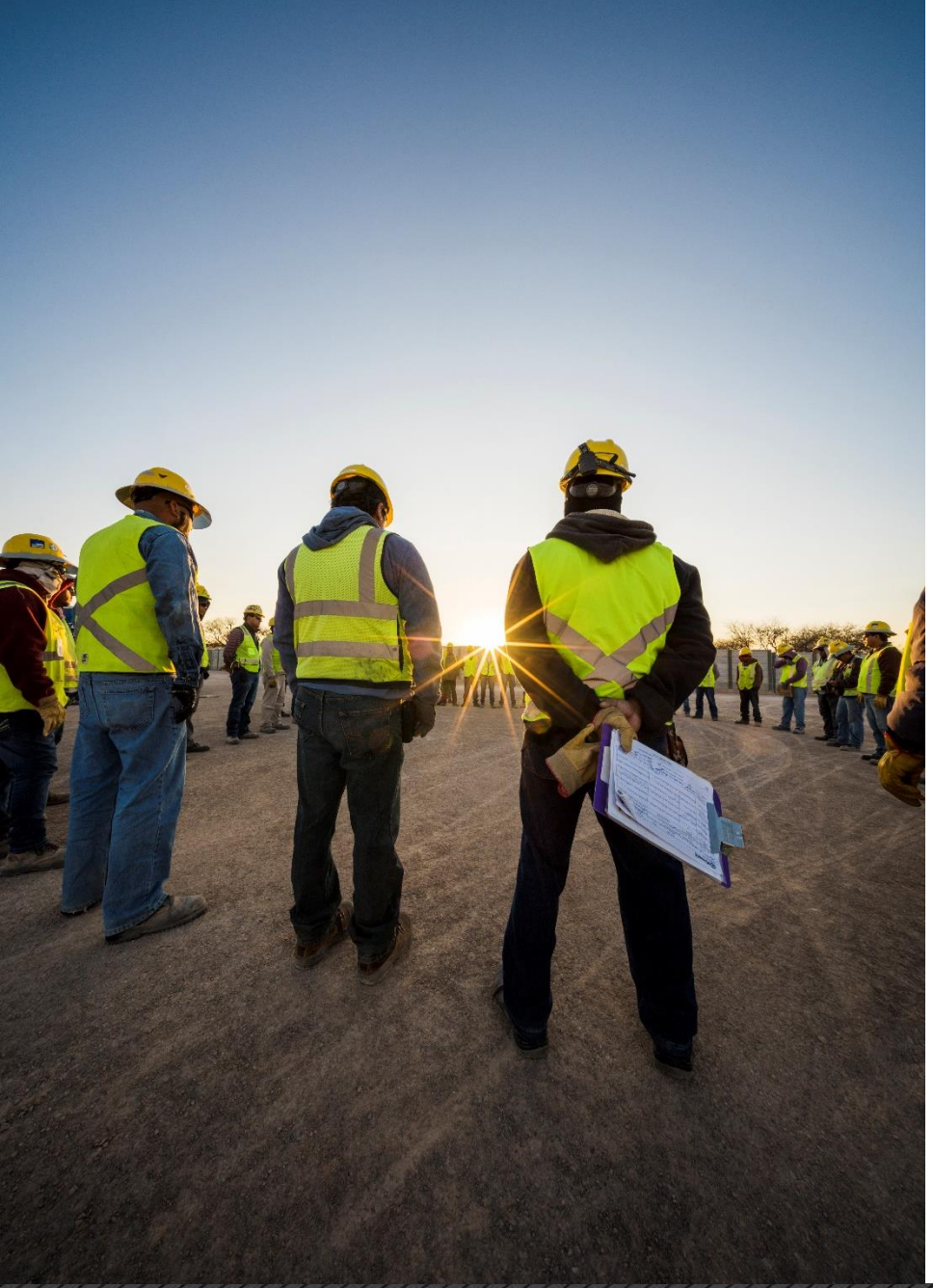


ZERO TO ISO 27001:2013

DAPHNE HOOVER AND BEN O'NEILL



AGENDA

Introduction

Our Story and Background

The Process

Life After Audit

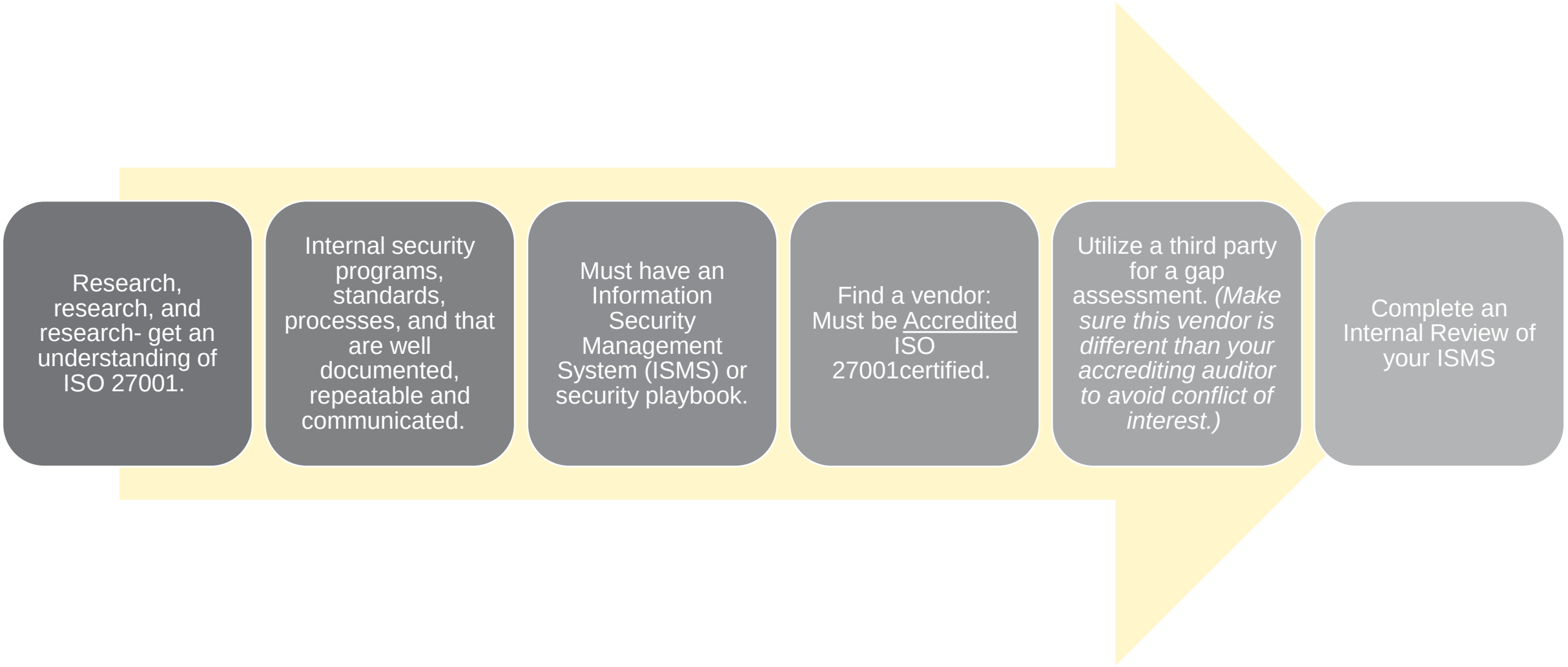
WHAT IS ISO 27001:2012?

- ISO 27001 is an international standard to manage information security
- Originally published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005.
- Revised in 2013 and again just recently in 2022.
- How many folks have or have worked for an employer that has ISO certification?
- What Industry?
- What team owns the ISO program at their employer? Internal Audit or Security.

OUR STORY AND BACKGROUND

- Late 2020 KTG Accomplished NIST CSF Attestation.
- Contracts requesting more proof of security controls.
- Negotiated 18-month lead for ISO 27001 certification.
- Real World occurrences changed Senior management purview.
  - Solar Winds
  - Colonial Pipeline
- Concerns from CISO to CEO.

THE PROCESS


Research, research, and research- get an understanding of ISO 27001.
Internal security programs, standards, processes, and that are well documented, repeatable and communicated.
Must have an Information Security Management System (ISMS) or security playbook.
Find a vendor: Must be Accredited ISO 27001certified.
Utilize a third party for a gap assessment. (Make sure this vendor is different than your accrediting auditor to avoid conflict of interest.)
Complete an Internal Review of your ISMS

STAGE 1 AUDIT

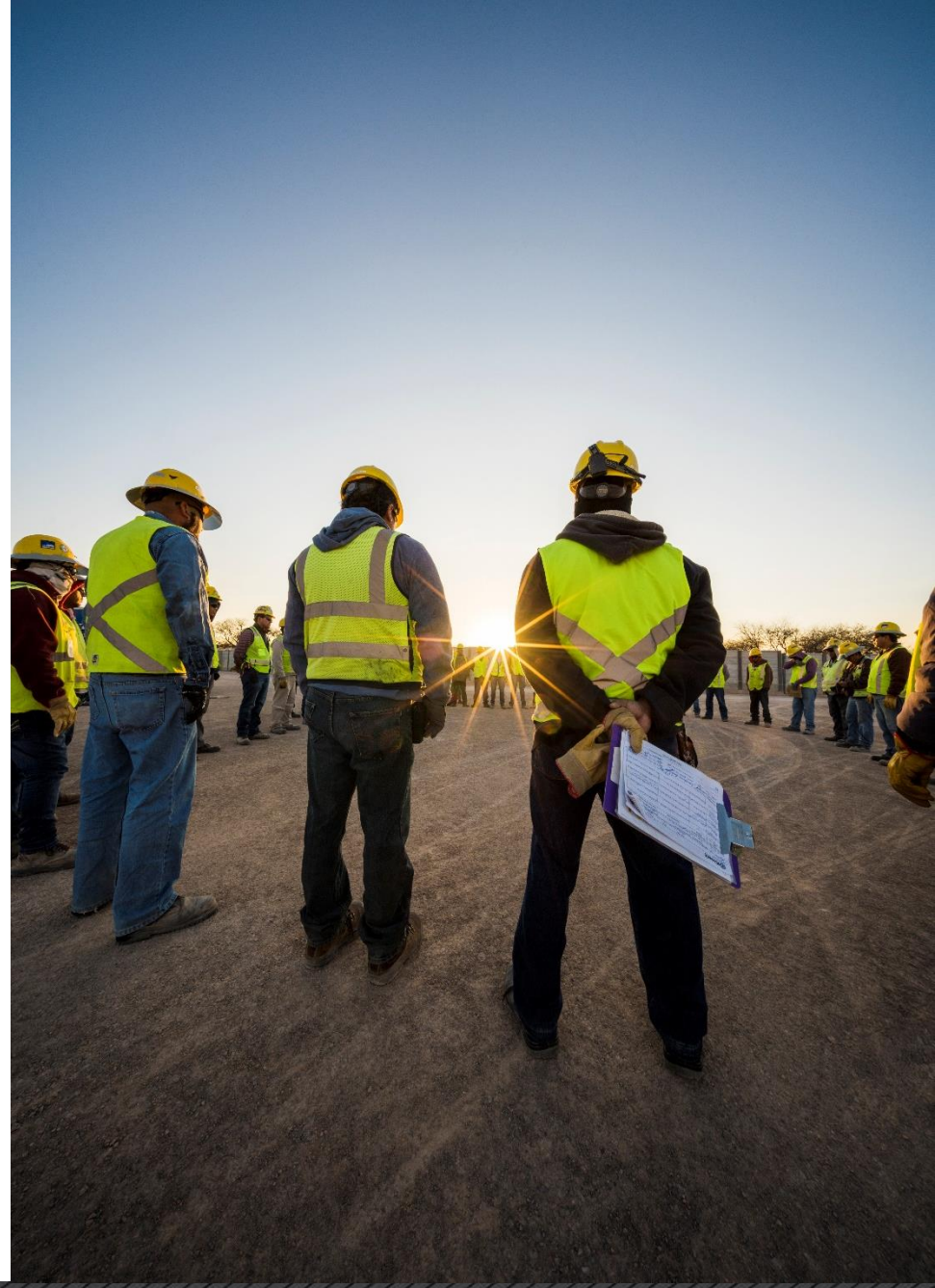
- The auditor will look for major nonconformities
- Automatic Failure:
  - No formal risk assessment conducted,
  - No Internal ISO audit review,
  - Incomplete or nonexistent statement of applicability and scope.
- The stage 1 audit consisted of a 4-5-hour conference call
- 40 items of documented evidence to be provided.
- A report identifying any areas of improvement issued by auditing firm.
- Plan of Action must be mapped out prior to initiation of stage 2.

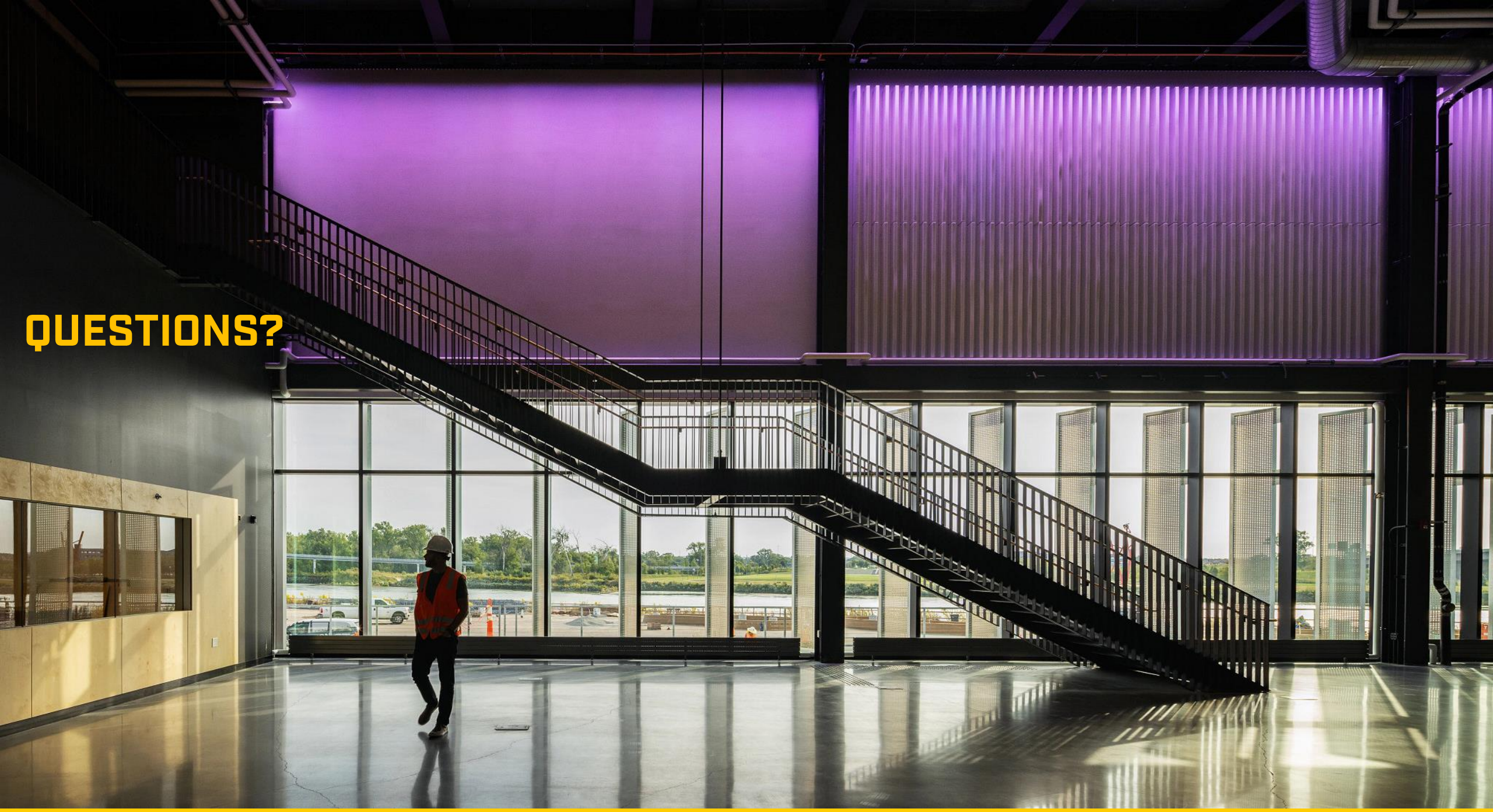
STAGE 2 AUDIT

- No more than 3 months from Stage 1 to address nonconformities.
- Stage 2 evaluates the implementation and effectiveness including effectiveness, of the Company’s ISMS.
- Required over 120 items of evidence to be delivered.
  - Documentation
  - Interviews
  - Screenshare
- Stage 2 report identifying any areas of improvement issued by auditing firm.
- Award of certification

AFTER THE AUDIT/CERTIFICATION

- Breathe, celebrate, get to work
- During the three-year lifespan of your ISO 27001 certification
  - Required annual internal audits of ISMS
  - Required annual external audits from your certification body
  - Year 1 – achieve Certification
  - Year 2 and 3 – Surveillance
- Continuous improvement to security program
- Worked with corporate communication teams to announce the achievement.
  - There are strict guidelines for displaying the cert and this can be audited by the ANAB.
- ISO 27001:2022




QUESTIONS?