

Review Article

Open Access

When Values Meet Targets: Designing Organizational Integrity Under Performance Pressure

Zvezdan Horvat

Adizes Institute Worldwide, Serbia

ABSTRACT

Organizations often respond to misconduct with more rules, training, and compliance staff, although major failures occur in firms that already possess these safeguards. This article defines organizational integrity as the capacity to maintain alignment among values, decisions, information, and conduct under performance pressure. Public records from Volkswagen, Boeing, Siemens, and Magyar Telekom reveal a recurring sequence: unbalanced targets, workarounds, silence, normalization, and exposure. The proposed integrity architecture rests on mutual trust and respect and six safeguards: clear boundaries, independent decision rights, balanced accountability, traceable information, protected voice, and verification with learning. It shifts attention from unethical individuals to organizations, where inconvenient facts can change decisions before failure becomes public.

*Corresponding author

Zvezdan Horvat, Adizes Institute Worldwide, Serbia.

Received: August 17, 2026; Accepted: August 21, 2026; Published: August 31, 2026

Keywords: Organizational Integrity, Ethical Culture, Compliance, Employee Voice, Behavioral Integrity, Adizes Methodology

Introduction

Codes matter, but they do not make an organization honest. Integrity is tested when a target is infeasible, a promise is endangered, or a manager prefers reassurance to unwelcome information. The question is whether the organization makes truthful conduct possible and consequential.

Behavioral integrity is alignment between words and actions [1]. Ethical leadership influences conduct through modeling, communication, reinforcement, and decisions [2]. Yet misconduct can become systemic without an order to break the law. Stretch goals narrow attention ethical fading removes the moral dimension from a technical choice and silence blocks corrective information [3-5]. Integrity is therefore an organizational capability, not only personal virtue or a compliance specialty.

This article asks: Which design conditions allow an organization to preserve integrity when commercial, technical, or political pressure makes truthful action costly?

Method

The study uses a theory-elaborating comparison of official public records. Cases were selected for contrast: Volkswagen concerns product and regulatory deception; Boeing concerns safety-critical design, certification, and manufacturing; Siemens concerns systemic foreign bribery; and Magyar Telekom concerns sham contracts and control circumvention. Evidence comes from the U.S. Environmental Protection Agency, the U.S. Department of Justice, the U.S. Securities and Exchange Commission, and the U.S. National Transportation Safety Board [6-12].

Each case was coded for objective, prohibited conduct, information behavior, authority, verification, exposure, and correction. The comparison identifies mechanisms rather than causal effects. Public records cannot reveal what every employee knew.

Comparative Evidence

Volkswagen installed software that detected emissions testing and altered vehicle behavior. U.S. authorities described a long-running scheme affecting approximately 590,000 vehicles [6,7]. Product success, compliance information, and verification were separated until deception became part of the product.

Boeing shows failure at several points in one value chain. In the 737 MAX case, technical information concerning the Maneuvering Characteristics Augmentation System was concealed from the FAA group responsible for pilot-training determinations [8]. After the 2024 Alaska Airlines 737-9 door-plug accident, the NTSB found that four securing bolts were missing, that there was no removal record, and that no required quality inspection had been performed. It also identified inadequate training and ineffective corrective action [9]. The events are distinct, but both show the danger of fragmented information, ambiguous closure, and weak verification.

At Siemens, U.S. authorities described falsified records and controls circumvented, followed by coordinated penalties totaling approximately \$1.6 billion in 2008 [10]. The company subsequently rebuilt its compliance system. Magyar Telekom used sham consulting contracts connected with Macedonia and Montenegro, showing how legitimate-looking documents can conceal prohibited purposes when controls are weak [11].

Across the cases, a difficult target creates pressure; a workaround removes the obstacle; information is narrowed; silence and short-

term success protect the workaround; repetition normalizes it; and an external event exposes the system. The objects differ, but the mechanism is similar.

Integrity as an Organizational Architecture

The foundation is mutual trust and respect. Trust without respect can become loyalty that suppresses disagreement; respect without trust can produce defensive formality. Together they legitimize professional challenge [13,14]. Six safeguards connect values to operations.

First, purpose and non-negotiable boundaries define what cannot be traded for revenue, schedule, or hierarchy. Second, decision rights separate proposal, approval, ratification, and verification when conflicts are material. Safety, compliance, and quality functions need access to decision-makers and protected stop-work authority. Third, accountability balances commercial results with quality, safety, compliance, and verified closure. Immediate rewards combined with delayed risk invite ethical discounting.

Fourth, critical information must be traceable from source to decision. Exceptions, altered assumptions, unresolved tests, and regulator-facing statements need ownership and an auditable path. Fifth, employee voice must be protected in practice. Managers should ask which facts would change a decision and whether their holders can speak safely. Sixth, verification must test reality independently and confirm that corrective actions work. Database closure is not elimination of recurrence. These safeguards turn culture into an operating system [12,15].

The safeguards reinforce one another. Voice without authority frustrates; authority without information becomes ceremonial; verification without consequences repeats findings. Integrity exists when accurate information can interrupt a target and trigger correction.

Managerial Implications

Leaders should begin with pressured decisions rather than another values campaign. For each high-risk decision, they should identify who proposes, decides, ratifies, verifies, and can stop implementation; which evidence cannot be overridden; how exceptions are recorded; and who confirms closure. Boards should examine recurring findings, incentive asymmetries, overdue actions, and issues that vanished without documented resolution.

Targets should be tested before commitment. When evidence makes a promise infeasible, the organization needs a legitimate route to change the target rather than the facts. Near misses and successful escalation deserve study because prevention is usually invisible.

Integrity is the capacity to preserve truthful conduct when targets, time, or authority creates pressure. Six mutually reinforcing design safeguards are:

- Purpose and boundaries. State what cannot be traded away for revenue, schedule, bonus, or status. Translate values into decision tests.
- Decision rights and ratification. Separate proposing, deciding, checking, and stopping high-risk work. Give independent expertise real authority.
- Targets and accountability. Balance commercial, quality, safety, customer, and long-term consequences. Reward escalation concealed success.

- Traceable information. Document exceptions, assumptions, changes, approvals, and unresolved risk. Make bad news difficult to erase.
- Voice and stop-work rights. Protect challenge, technical dissent, and escalation across the hierarchy. Respond without retaliation or delay.
- Verification and learning. Use independent testing, audit, and board review; repair causes, not optics. Test whether controls work in practice.

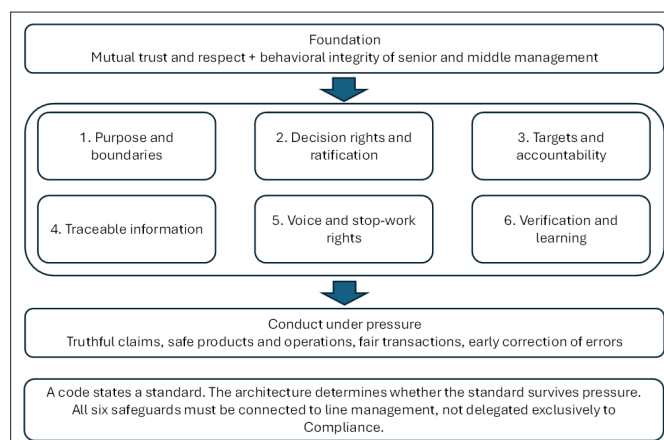


Figure 1: Organizational Integrity Architecture

Source: Author's synthesis based on Adizes, Edmondson, Kaptein and the comparative cases [13-15].

Limitations and Conclusion

The comparison uses a small, purposefully selected set of public failures. It cannot measure prevalence or isolate culture from technology, regulation, and markets. Future research should study high-risk decisions prospectively and compare failures with organizations that corrected problems before exposure.

Integrity is not the absence of bad people. It is a pattern of choices, information, authority, incentives, and verification that determines whether truth remains actionable under pressure. The cases show how ordinary processes normalize extraordinary risk. Organizations become more trustworthy when purpose sets boundaries, authority is balanced, information is traceable, dissent is protected, and correction is independently verified. Values matter most when the system permits them to defeat the target.

Declarations

Funding: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of interest: The author declares no conflict of interest.

Data availability: All public-case materials are identified in the reference list.

Use of generative AI: A generative AI tool was used to support literature discovery, synthesis, language editing, figure construction, and document preparation. The author is responsible for verifying all claims, citations, translations, and the final manuscript in accordance with the journal's policy.

References

1. Simons T (2002) Behavioral integrity: the perceived alignment between managers' words and deeds as a research focus. *Organ Sci* 13: 18-35.
2. Brown ME, Treviño LK, Harrison DA (2005) Ethical leadership: a social learning perspective for construct development and testing. *Organ Behav Hum Decis Process* 97: 117-134.
3. Ordóñez LD, Schweitzer ME, Galinsky AD, Bazerman MH (2009) Goals gone wild: the systematic side effects of overprescribing goal setting. *Acad Manag Perspect* 23: 6-16.
4. Tenbrunsel AE, Messick DM (2004) Ethical fading: the role of self-deception in unethical behavior. *Soc Justice Res* 17: 223-236.
5. Morrison EW (2014) Employee voice and silence. *Annu Rev Organ Psychol Organ Behav* 1: 173-197.
6. US Environmental Protection Agency (2026) Learn about Volkswagen violations [Internet]. Washington (DC): US Environmental Protection Agency <https://www.epa.gov/vw/learn-about-volkswagen-violations>.
7. US Department of Justice (2017) Office of Public Affairs. Volkswagen AG agrees to plead guilty and pay \$4.3 billion in criminal and civil penalties; six Volkswagen executives and employees are indicted in connection with conspiracy to cheat U.S. emissions tests Washington (DC): US Department of Justice. <https://www.justice.gov/archives/opa/pr/volkswagen-ag-agrees-plead-guilty-and-pay-43-billion-criminal-and-civil-penalties-six>.
8. US Department of Justice (2021) Office of Public Affairs. Boeing charged with 737 MAX fraud conspiracy and agrees to pay over \$2.5 billion Washington (DC): U.S. Department of Justice. <https://www.justice.gov/archives/opa/pr/boeing-charged-737-max-fraud-conspiracy-and-agrees-pay-over-25-billion>.
9. National Transportation Safety Board (2024) In-flight separation of left mid exit door plug, Alaska Airlines Flight 1282, Boeing 737-9, N704AL. Washington (DC): National Transportation Safety Board; 2025 Jun 24. Aviation Investigation Report AIR-25-04. <https://www.nts.gov/investigations/AccidentReports/Reports/AIR2504.pdf>.
10. US Department of Justice (2008) Office of Public Affairs. Siemens AG and three subsidiaries plead guilty to Foreign Corrupt Practices Act violations and agree to pay \$450 million in combined criminal fines Washington (DC): US Department of Justice. <https://www.justice.gov/archive/opa/pr/2008/December/08-crm-1105.html>.
11. US Securities and Exchange Commission (2011) SEC charges Magyar Telekom and former executives with bribing officials in Macedonia and Montenegro Washington (DC): US Securities and Exchange Commission. <https://www.sec.gov/news/press/2011/2011-279.htm>.
12. US Department of Justice (2024) Criminal Division. Evaluation of Corporate Compliance Programs [Internet]. Washington (DC): US Department of Justice. <https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl>.
13. Adizes I (1992) Mastering change: the power of mutual trust and respect in personal life. family life, business and society. Santa Monica (CA): Adizes Institute. https://www.goodreads.com/book/show/300021.Mastering_Change.
14. Edmondson AC (1999) Psychological safety and learning behavior in work teams. *Adm Sci Q* 44: 350-383.
15. Kaptein M (2008) Developing and testing a measure for the ethical culture of organizations: the Corporate Ethical Virtues model. *J Organ Behav* 29: 923-947.

Copyright: ©2026 Zvezdan Horvat. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.