The Use of Rule Languages for Policy and Legal Compliance

Jeffrey B. Ritter

jritter@klng.com

The Challenges

- Compliance, governance and data transparency are imposing compelling pressure to produce demonstrable, data-based evidence of performance.

- Public policy is increasingly anticipating that IT resources can be employed to achieve policy-based obligations.

- Interoperability demands of the “extended enterprise” currently expose businesses to inefficient and risk-intensive means of expressing controls reflecting rule-based requirements.

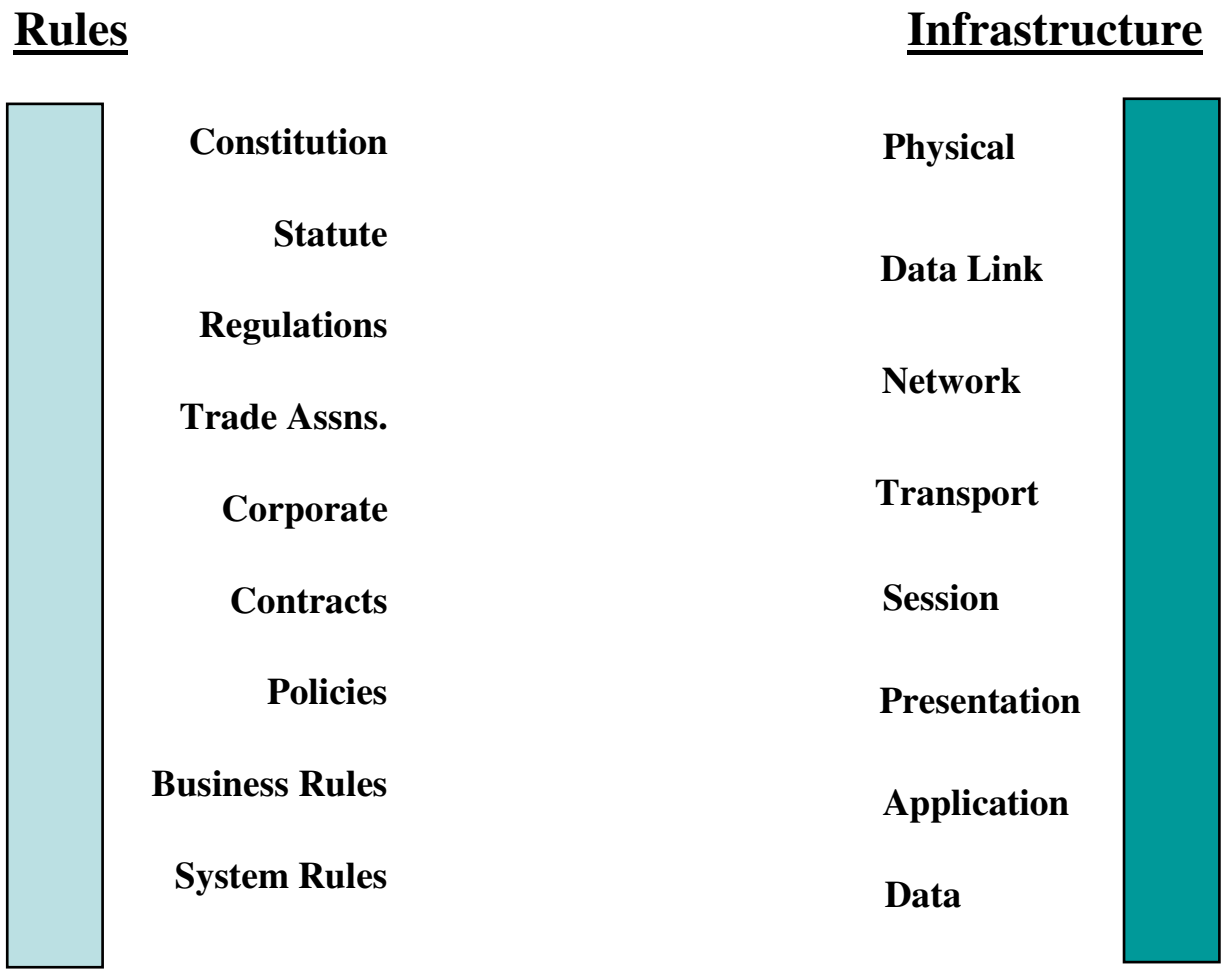
Corporate Governance

- **Sarbanes-Oxley—the adequacy of internal controls**
- **Basel II—managing operational risk (to achieve increased capital availability)**
- **The Compliance Rule (for Mutual Funds)**
- **The NASD Certification Rule**

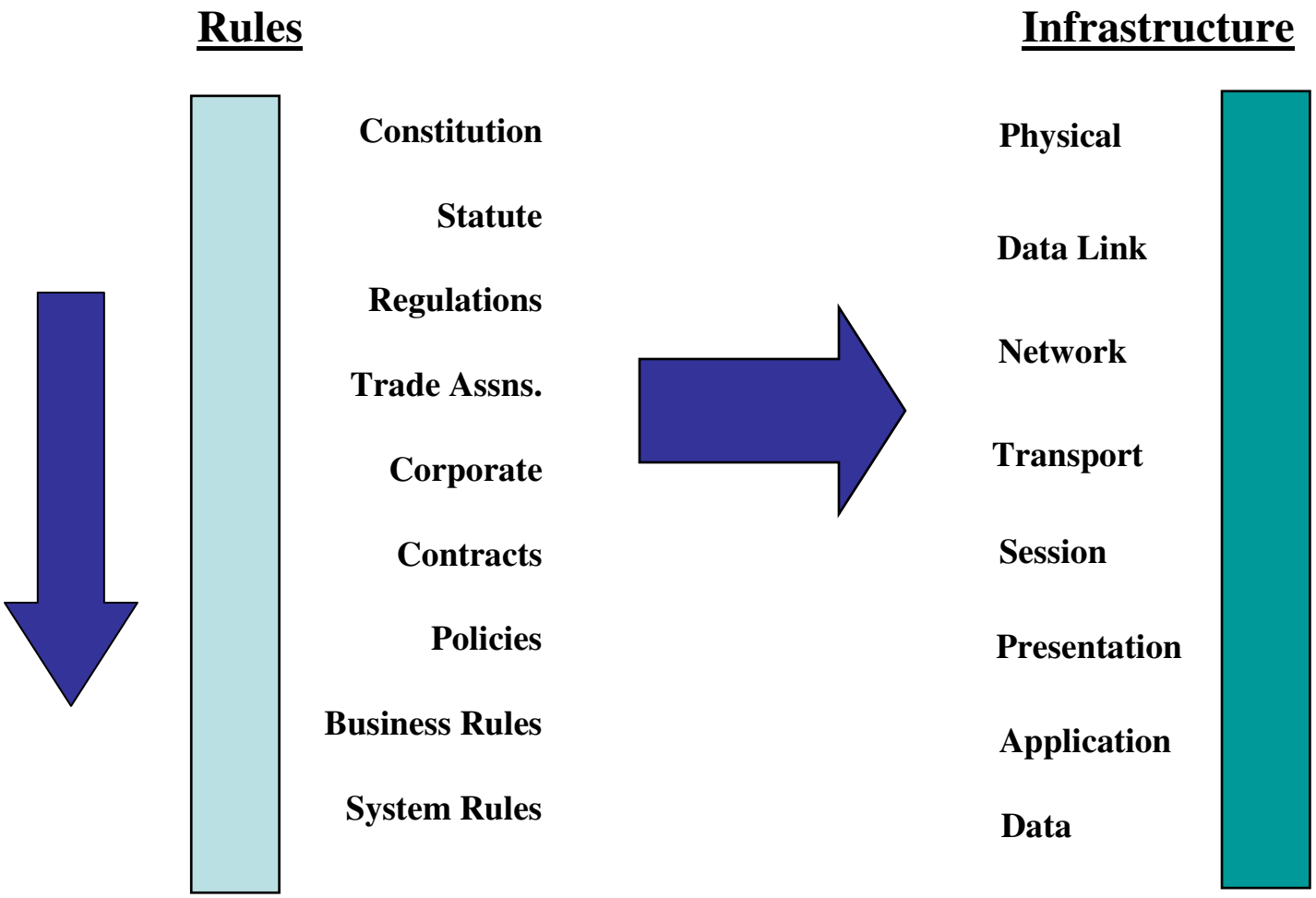
That which is not recorded did not occur.
That which is not documented does not exist.
That which is not approved and audited is vulnerable.

"The company must be able to document, to an objective reviewer, that compliance has occurred in fact."

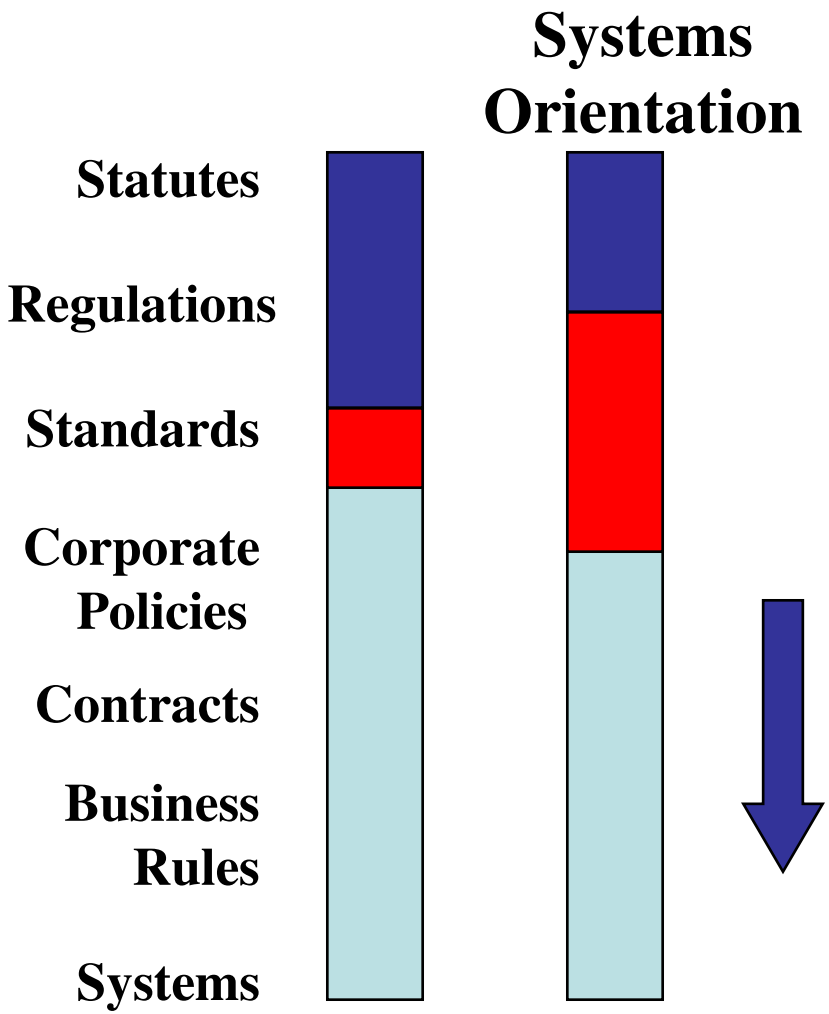
A “legal” view of governance



Implementing Business Rules



Rapid Evolution is Occurring



- Formal law is compressing
- Increased reliance on standards
- Increased expression of corporate governance in systems and controls

Proposed Use Cases

1. Vulnerability testing/software quality control
   - Express software design requirements, both for normative “best practices”/required elements and customized requirements.
   - Perform validation of the use of design controls to achieve requirements.
   - Facilitate improved trust in the acquisition and integration of code assets into operations (particularly extended enterprise).

Proposed Use Cases

2. Information Security Controls

--Develop “communities” and “collections” that facilitate reliable expression of requirements while retaining flexibility for unique controls.

--Express requirements in a manner that produces demonstrable evidence of compliance with “legal” requirements.

--Produce more rapid implementation of ISO17799/BS 7799 requirements with higher trust value in the implementation of controls.