



IT Controls Benchmarking Survey

Quantifying The Value, Effectiveness,
Efficiency and Security of IT Controls
(Formerly known as “VEESC Survey”)

August 15 Status Report



- Background
- Problem statement
- Hypotheses
- Methodology
- Preliminary findings
- Next steps



Background - ITPI

- The IT Process Institute (ITPI), is not for profit organization that exists to support the membership of IT audit, security, and operations professionals.
- Our mission is to advance IT management science through independent research, benchmarking, and prescriptive guidance.
- Our vision is to identify and study top performing IT organizations to create evidence based best practices that enhance the efficiency and effectiveness of member organizations.



Background - Researchers

- Rohit S. Antao
 - Information Networking Institute and CERT/SEI, Carnegie Mellon Univ.
- Kevin Behr
 - CTO, IP Services
 - Director of Prescriptive Guidance, ITPI
- Grant Castner
 - Assistant Professor, University of Oregon
 - Director of Benchmarking, ITPI
- Gene Kim
 - CTO, Tripwire
 - Director of Research, ITPI
- Andrew P. Moore
 - CERT/SEI and CyLab, Carnegie Mellon University



Background - Objectives

- To provide statistically valid evidence that IT controls do improve the efficiency and effectiveness, of IT operations.
- Allow organizations to benchmark themselves against high performers.



Problem statement

- IT management is almost universally tasked with:
 - Deliver adequate availability, contain costs, maintain adequate security, comply with regulations, attest to effective controls.
- When IT management cannot bring quantitative science to bear on these problems, what often results is:
 - Failed initiatives and projects,
 - Increased suspicion from the business,
 - Pressure to outsource,
 - Inability to get additional capital for future projects,
 - Difficulty in even justifying the existence of IT,
 - Short tenures for IT executives.



Problem statement

- The real tragedy for the industry is that without understanding why IT management actions fail:
 - IT executives and the business are doomed to lonely efforts of trial-and-error to figure out how to achieve success the next time around.
 - IT executives and the business are at the mercy of consultants and popular trade press that use circumstantial evidence to recommend the “next thing to try.”



General hypotheses

- Some IT controls improve IT process efficiency and effectiveness.
- We also hypothesize that:
 - Not all controls are equal
 - That change management controls and access management controls are the dominant controls.
 - Without these controls, other controls (e.g. in problem and release management) will be less effective.
 - Unplanned work is an effective indicator of poor service levels and uncontrolled change.



VEESC research questions

1. What are the effectiveness and efficiency characteristics of high-performing IT operations organizations?
 - What controls and processes make them different from typical IT organizations?
 - What management belief systems are common to them?
2. What are the financial benefits of high performance?
3. Can we prove the business value of certain IT practices so that controls can be owned by IT management, instead of being forced upon them by audit?

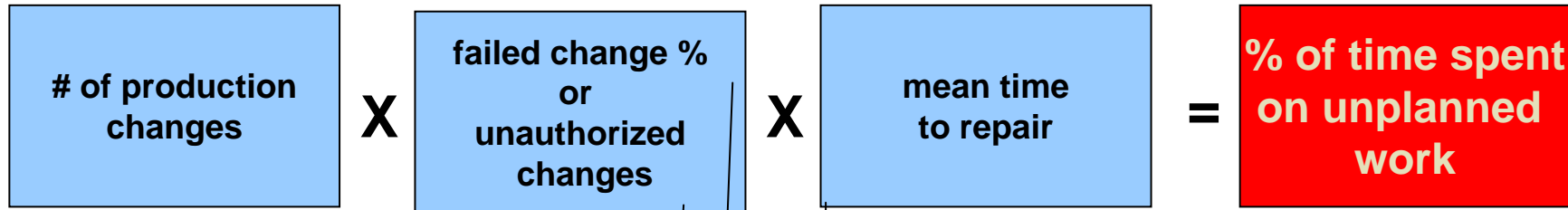


Methodology

1. Dr. Grant Castner at the University of Oregon is facilitating the actual survey. He is using Structural Equation Modeling – to find statistically relevant correlations between behavior and performance.
2. Andrew P. Moore and Rohit S. Antao of Carnegie Mellon University will then use Systems Dynamics Modeling to model the causal mechanisms to identify specific behaviors that differentiate top performers.
3. The ITPI in conjunction with these research institutes will then study specific top-performers.
4. The ITPI will then publish prescriptive guidance related to these findings.



Measuring effectiveness and efficiency



Behaviors that **increase** change **success** rate:

- Effective change testing
- Effective risk review when approving changes
- Effective identification of change stakeholders
- Effective change scheduling

Behaviors that **reduce unauthorized changes**:

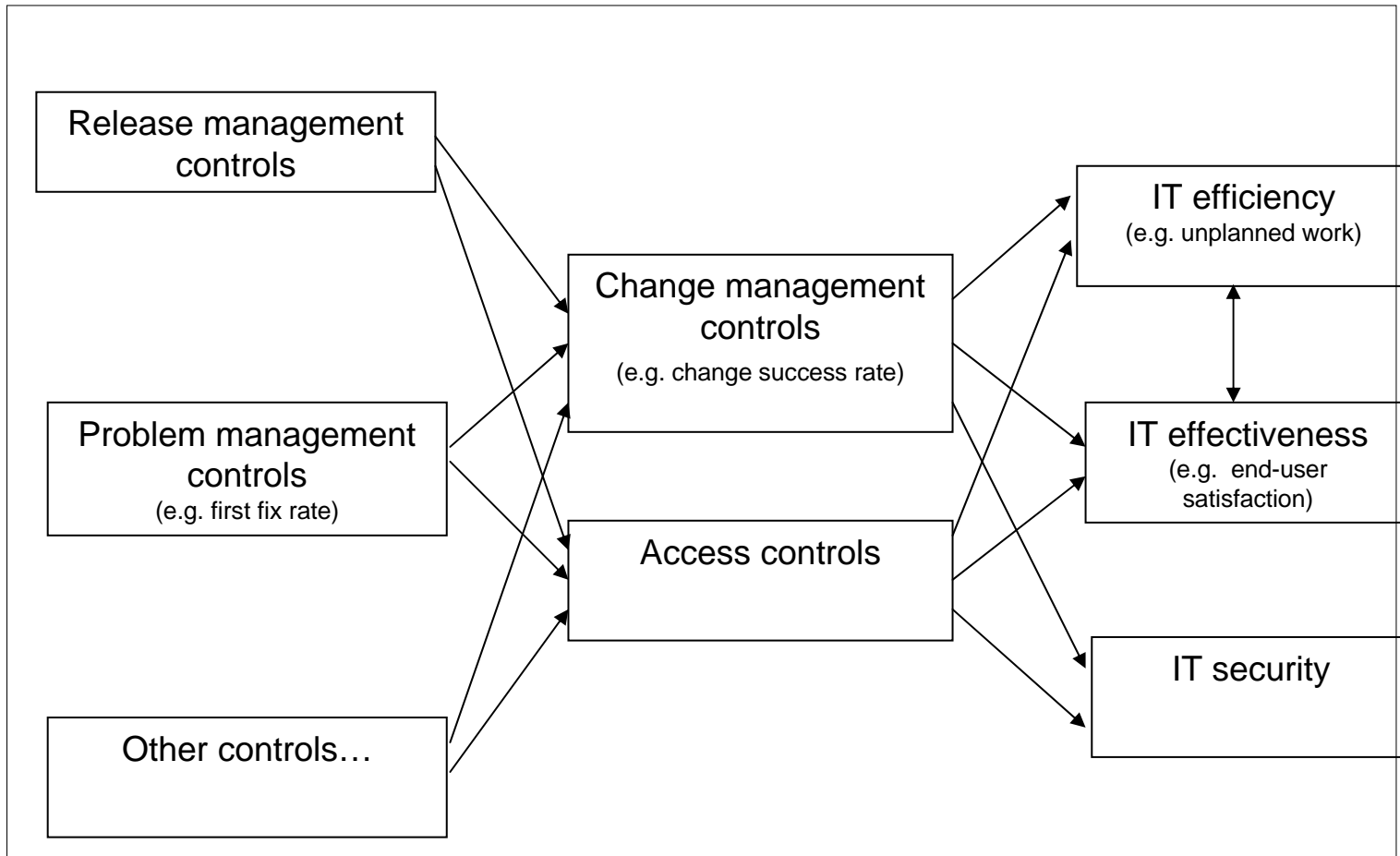
- Culture of change management
- Management ownership of change process
- Effective monitoring of infrastructure with detective controls to enforce change process
- Management use of corrective action when change processes are not followed.

Behaviors that **decrease** MTTR:

- Culture of causality: desire to rule out change first in problem repair cycle
- Effective change management process that can report on authorized and scheduled changes
- Ability to distinguish planned and unplanned outage events
- Effective communications around scheduled changes
- Effective monitoring of infrastructure for production changes



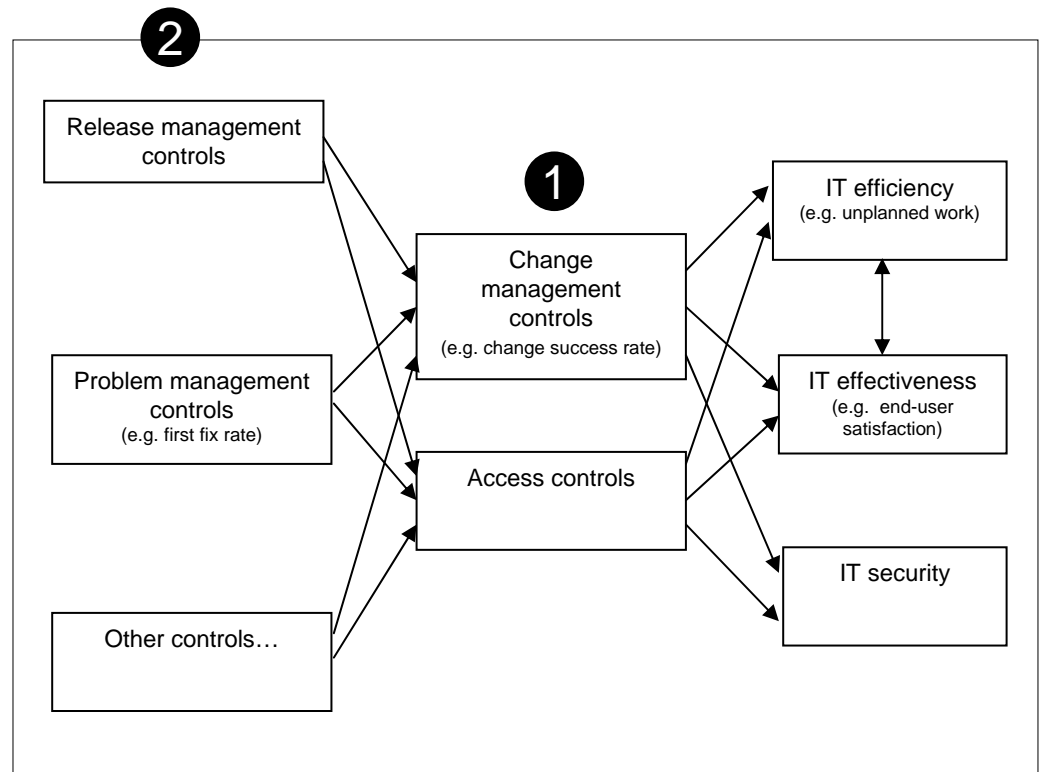
Structural Model





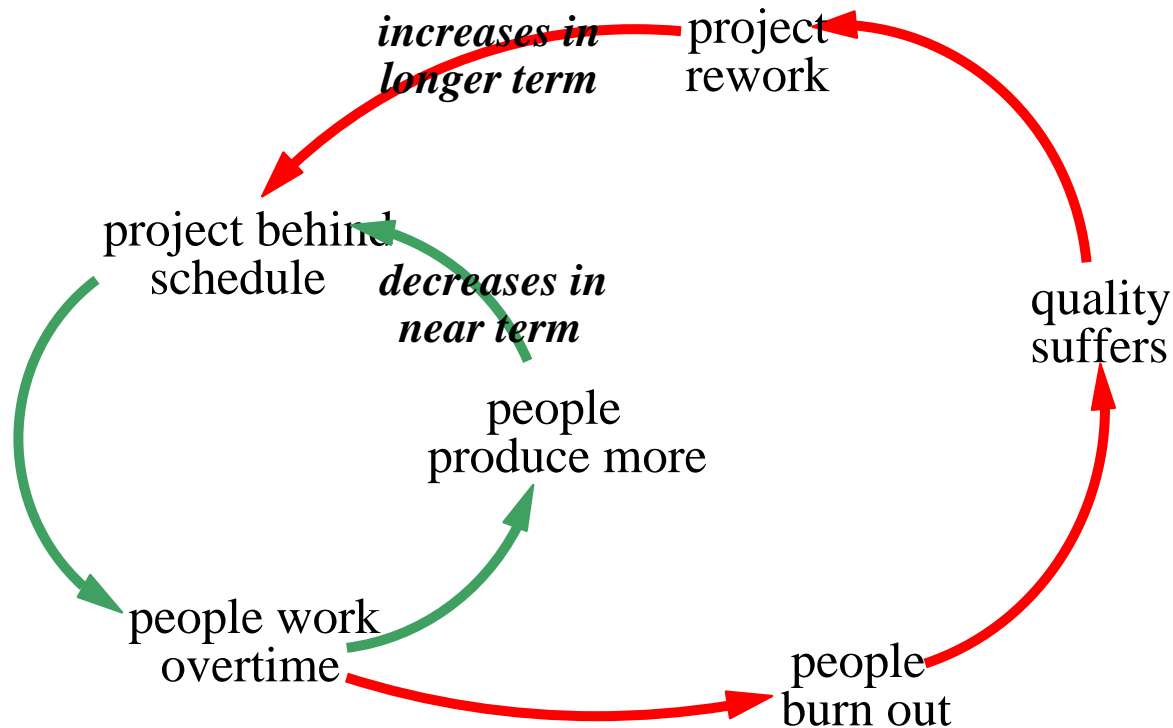
Reading The Structural Model

1. Change management controls directly affect IT efficiency/effectiveness/security
2. Release management controls affect IT efficiency/effectiveness/security, but only in the presence of change management controls





Systems Dynamics Model – simple example

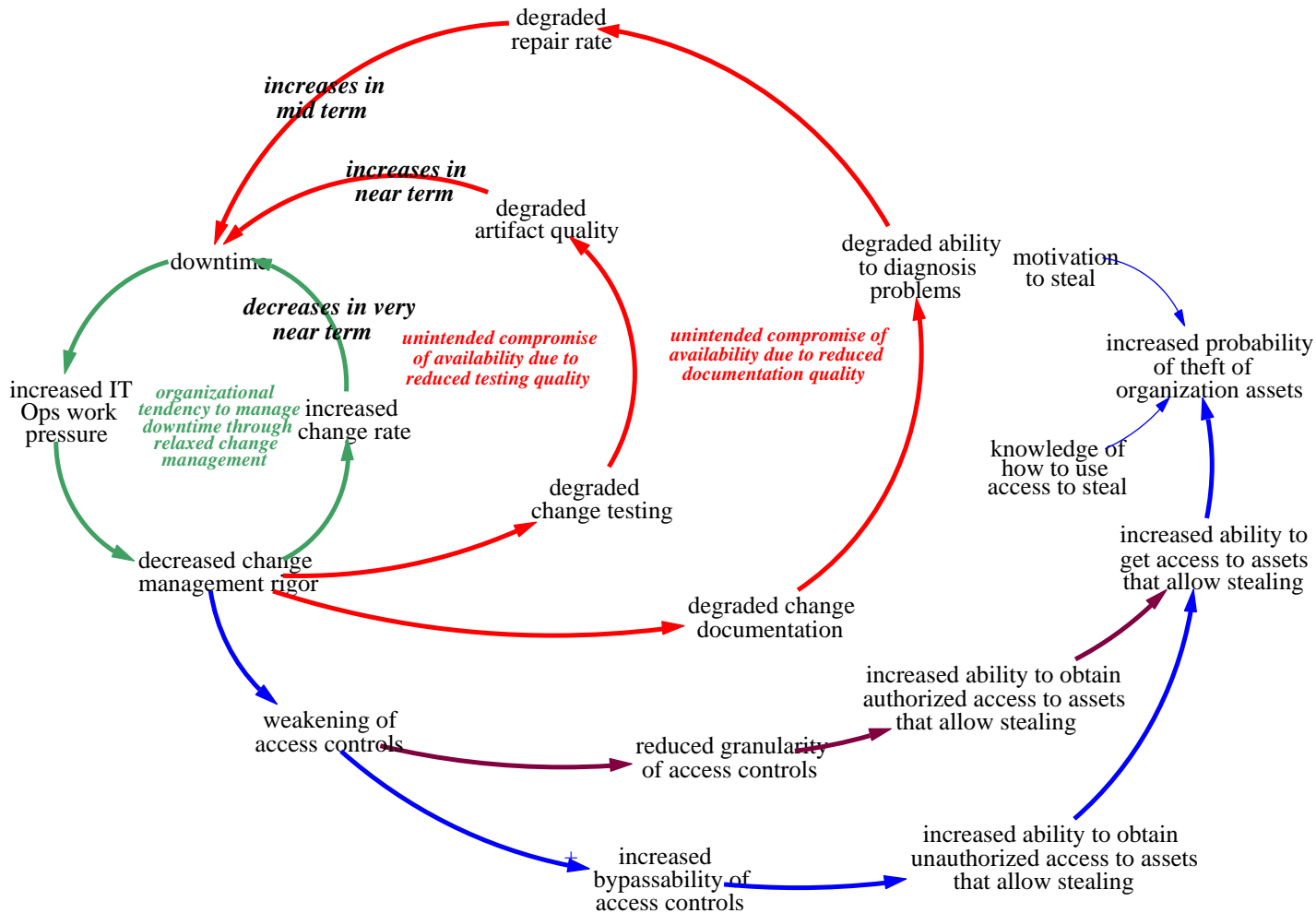


* Notation used simplifies SD syntax to ease explanation.

Source: Rohit Antao, Andrew Moore - Carnegie Mellon University

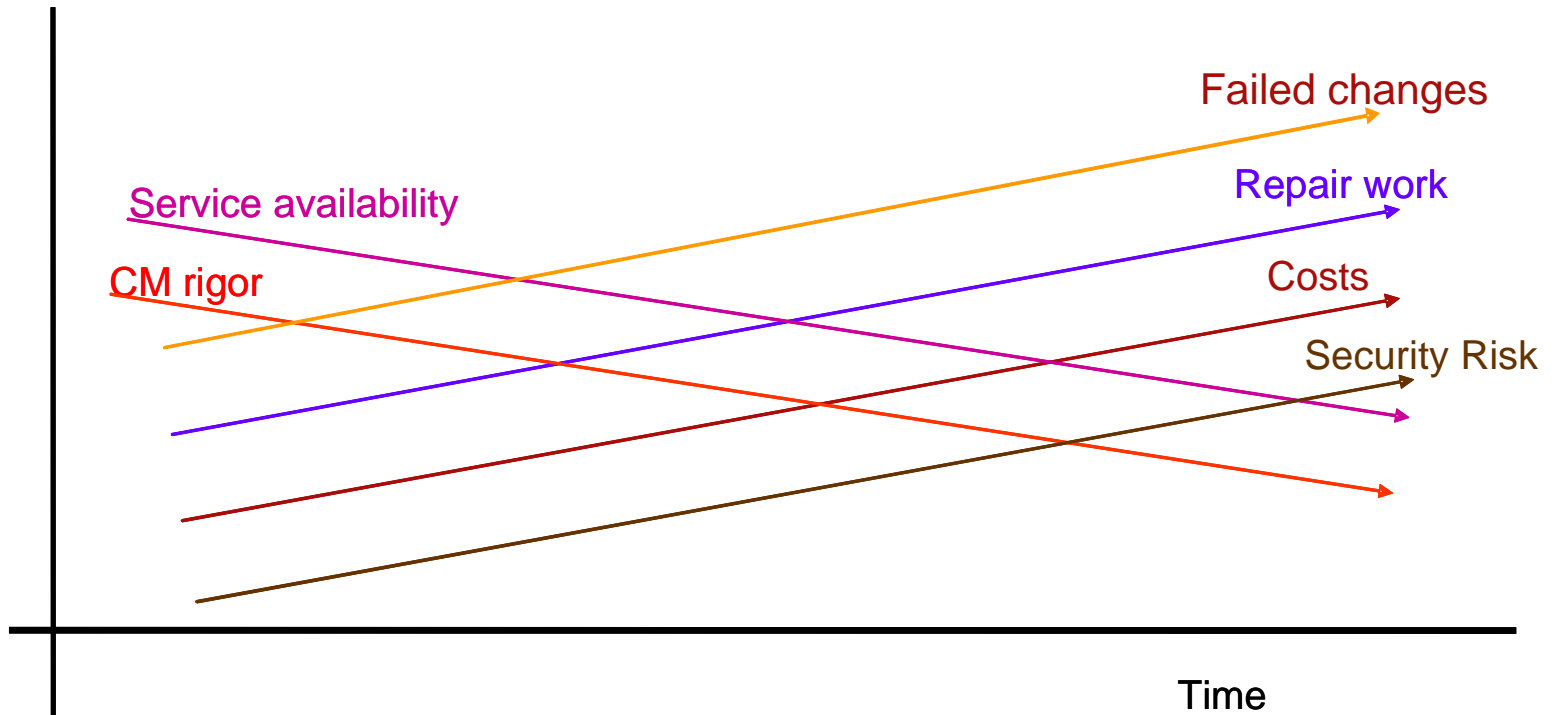


Systems Dynamics Model – Preliminary Example





Problem Behavior over Time: The Reference Mode



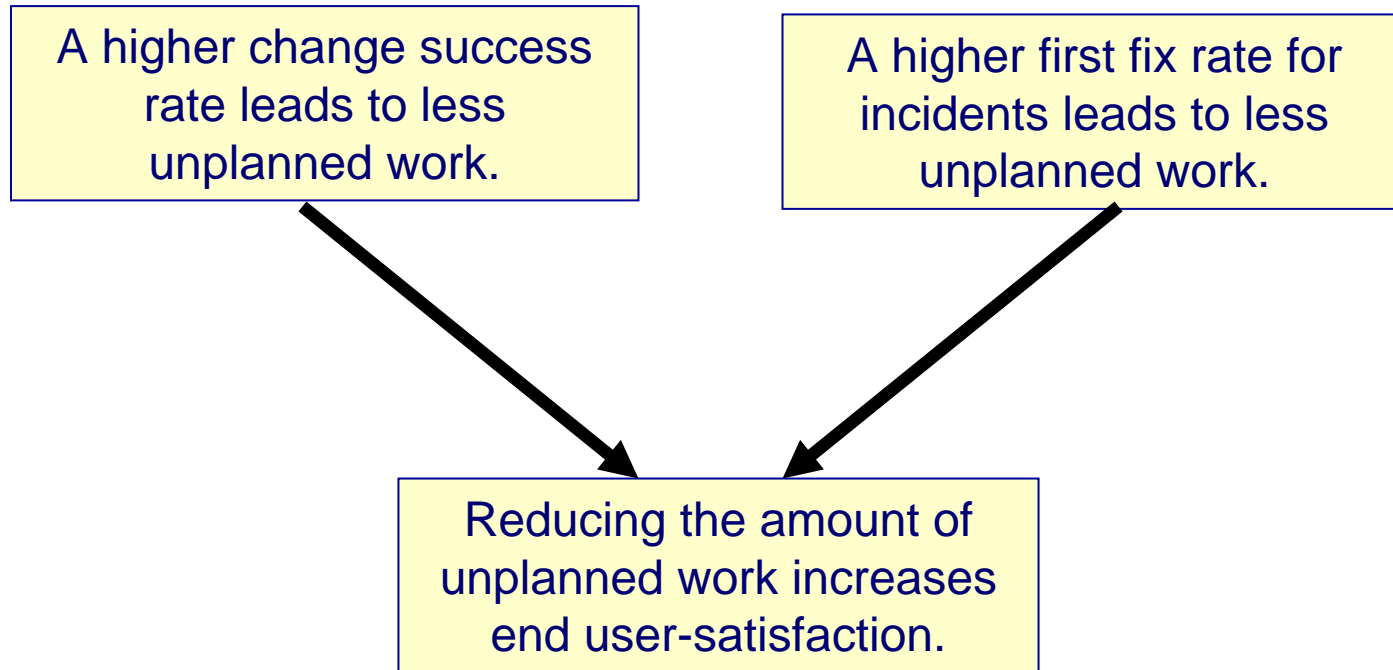


Preliminary findings

- The change success rate is negatively correlated with the unplanned work rate.
- Unplanned work rate is negatively correlated with the percentage of problems fixed on the first attempt.
- The unplanned work rate is negatively correlated with the IT department's perception of end-user satisfaction.



Preliminary conclusions





Next Steps

- Continue analysis of other controls to analyze their affect on IT effectiveness, efficiency, and security.
- Increase survey participation to to improve the statistical significance of the results.
- Feed results to Carnegie Mellon Software Engineering Institute to validate and refine their Systems Dynamics Model