Design Patterns for Compensating Controls for Securing Financial Sessions

Marc Dupuis
Computing and Software Systems
University of Washington
Bothell, Washington, U.S.A.
marcjd@uw.edu

Camelia Bejan
School of Business
University of Washington
Bothell, Washington, U.S.A.
cameliab@uw.edu

Matt Bishop
Department of Computer Science
University of California Davis
Davis, California, U.S.A.
mabishop@ucdavis.edu

Scott David
Applied Physics Laboratory
University of Washington
Seattle, Washington, U.S.A.
sldavid@uw.edu

Brent Lagesse
Computing and Software Systems
University of Washington
Bothell, Washington, U.S.A.
lagesse@uw.edu

***Abstract*—We formally extend the processes of design patterns from software engineering into the area of session management and transactional risk management, in an effort to improve the reliability, predictability, and security in identity. This work addresses identity management systems that sustain sessions across extended supply chains of multiple technologies and policies. The design patterns will help promote better practices in the design and development of these session-management and transaction-management systems, and the overview of compensating controls will record common practices in addressing the inconsistencies faced by real-world systems in working across technical and policy domains. An initial design pattern for compensating controls was developed. It addresses purchasing products or services from a web merchant with PCI DSS serving as the backdrop for existing controls and for which compensating controls might be needed. The approach used for this initial design pattern for compensating controls may be used in other areas so that a repository of these documents may be available to various stakeholders to provide more secure and robust systems. Likewise, the holistic approach employed here by incorporating multiple perspectives–business, legal, and technical–provides a useful framework for addressing the organizational realities of deploying and protecting information systems from various threats.**

***Index Terms*—compensating controls, design patterns, financial sessions, security, privacy, confidentiality, economic, legal, business, technical**

I. Introduction

Among the many risk-related decisions made by an organization are those decisions on how to deal with identity-related risks of various sorts. Actively managing risk when it comes to authentication and access control requires an organization to make choices to avoid, mitigate or accept various identity, session, and transactional behavior risks, and to make those choices in the context of other organizational risks.

Current practices are to a great extent focused on mitigating identity risk by ensuring the use of consistent, standardized approaches such as levels of assurance and authentication strength of tokens. It is currently left up to service providers to develop unique and custom approaches to managing session and transactional behavior risk by the use of compensating controls such as additional system controls, architectures, default states, constraints, etc. that are applied in session and transaction contexts to compensate for sources of insecurity that would otherwise be unaddressed. Where organizations are forced to create their own customized compensating controls, interoperability, scalability, and ultimately security suffer. Mistakes are made by organizational insiders, even when their intentions are not malicious [4].

The situation is made worse by the fact that identity management-based (IdM-based) security risks associated with session management are not currently extensively cataloged or standardized. The result is that these system elements cannot be easily referenced, communicated or applied by and among developers and other IdM stakeholders. This results in duplication of effort, solutions that cannot scale, lack of interoperability across and among systems, increased costs of design, development and deployment, and an overall net negative impact on IdM system integrity, reliability and security.

Unfortunately, system security can also be compromised by additional threats, and external and internal vulnerabilities that arise after an identity credential is issued, and even after a party is authenticated in a system. Those additional risk profiles arise because sessions and transactional activities involve the dynamic use of, application of, and reliance upon, IdM, which introduces exposure to additional threats and vulnerabilities that emerge in those IdM-in-use scenarios.

Our focus is on design patterns for compensating controls associated with sessions management and transaction management systems, both of which are settings in which identities, credentials, and claims are presented and relied upon by stakeholders to minimize the risks involved with interactions. This focus is based on the observation that the standards and

This project was sponsored by the U.S. Department of Homeland Security, Science & Technology Directorate.

practices for systems that support these aspects of *IdM in use* are underdeveloped relative to the processes associated with issuance and maintenance of identity and credential tokens and other similar *pre-use* identity processes.

Our project expanded the design patterns processes (and compensating controls applications of those patterns) with a focus on security design patterns of identity-in-use and specifically in the case of its use in the dynamic and real world contexts of sessions management.

An initial design pattern for compensating controls was developed. It addresses purchasing products or services from a web merchant with PCI DSS serving as the backdrop for existing controls and for which compensating controls might be needed.

II. Background

Design patterns have been used extensively and successfully in software development [3], [5], [9]–[11]. This has permitted software architectural practices to be semi-formalized, allowing them to be more readily conveyed among developers and practitioners, enhancing design efficiency and interoperability at the architectural level (see Hoekstra et al. [6]).

Our project developed an initial design pattern for the context of session management for financial transactions, which remains under-developed despite significant efforts [1]. Future efforts will focus on identifying and cataloging additional design patterns that apply across multiple technologies working together to provide sessions management and interaction management for banking and financial systems (see below). This type of development context calls for a "systems of systems" approach that can be applied among different technologies brought together in extended and hybrid supply chains that support many commercial and governmental IdM systems and information management systems.

To the extent that financial market identity systems are recognized as being built from hybrid stacks of independent technology, business and legal layers, this first portion of the project focused on design patterns that emerge horizontally among technologies within the technology layer of the hybrid stack. This perspective is an important foundation of our work to identify and map compensating controls that can be applied among technologies to mitigate sessions and transactional risks. Our initial design pattern also shows how to apply design patterns vertically connecting the hybrid business, legal, and technical stacks.

A. Design Patterns Applied in Law and Policy

The concept of patterns and its application in developing standards and practices is not limited to software development. In fact, it is highly developed in law, even though it has a different name. In the context of legal rules development (either in public laws and regulations or in private contract), pre-law design patterns are frequently called "customs". There is a rich body of research on the processes by which customary patterns of behavior become formalized into enforceable duties by contract or legislative or regulatory action. The processes are roughly similar to that applied in software development, revealing legal work to ultimately involve a form of behavioral engineering and interaction programming. Just as design patterns provide informal guidance relating to the programming of a particular software application, so too do patterns of legal rights and duties offer informal guidance for new drafting solutions (see Bederman [2]).

B. Patterns Applied in Economic Decisions

A third driver of socio-technical systems performance is economic considerations and motivations. In this context, "economic" refers to the value-based considerations (monetary and otherwise) that affect individual and institutional decisions, as well as the variety of potential types of incentives and penalties that can be applied to help guide behaviors toward reliability and predictability. In fact, while the performance of socio-technical systems such as IdMs are clearly guided by technical, legal and economic drivers, it is ultimately the economic drivers that provide the dominant causative relationship to the performance of stakeholders acting within those systems, and in the aggregate to the performance of the overall system. This project sought to discern and then apply the design patterns of effective incentives and penalties as compensating controls to help meet the challenges of improving the integrity of identity management systems deployed in support of mitigating sessions and transactional risks and vulnerabilities.

C. Limitations of Current Efforts

Design patterns for compensating controls have demonstrated significant value in making technical systems more reliable. For IdM solutions, however, the focus has historically been on designing and developing technical solutions in isolation from other technical systems, and also in isolation from other non-technical system elements with which they must interact in real world deployments and uses (such as sessions and transactional settings).

The problem of isolation of technical components from one another is starting to be addressed in labs and mock-up environments where technical systems can be tested and tuned for greater interoperability with other technical systems. Our work helps extend the design patterns work among technologies to cover the extended (and frequently federated) IdM service "supply chains" that come together in sessions and transactional management and security.

We also addressed the latter problem — that of isolation of the technology design, development and testing from real word settings. In those real world settings, system performance is driven by technology and economic and legal considerations. We demonstrate, through "patterns handbooks" and sample "trust frameworks" that describe and document hybrid compensating controls, how hybrid design patterns can improve identity management to mitigate sessions and transactional and behavioral risk.

III. Approach

We developed a basic ontology and applied it to purchasing products or services from a web merchant. This preliminary work validated that the ontology correctly captured the critical elements and key components of this design pattern. This initial design pattern was done within the context of existing controls — PCI DSS — that represent a hybrid combination of technical, legal, policy, economic, and business controls to mitigate risk. This was done so that instead of working with two unknowns — existing controls and design patterns with associated compensating controls — we instead worked with one known (existing controls) so that we may be able to validate and focus our attention to the unknown (design patterns with associated compensating controls). We felt this was important in our initial design pattern so we would remain focused on the factors relevant for the work being done in this initial phase. In other contexts (i.e., other types of online financial transactions), PCI DSS will not apply.

The ontology captured representations of security implementations and approaches for financial transaction systems at several levels. Thus, we will be able to reason at any desired layer of abstraction, and (ideally) among the different layers. This will also allow us to tie the compensating controls to different layers of abstraction, and validate the relationships among the compensating controls at the specification, design, and implementation and operation levels. It will also allow us to compare compensating controls at different levels, and where commonality among these are found, derive new design patterns. Finally, it will allow implementers of these security systems to take into account what compensating controls to add when given the desired higher-level compensating controls. Ultimately, we are seeking to streamline and improve the processes for design, development and deployment of IdM security systems for session management.

We have also shown how certain approaches for securing online financial transactions can be reinterpreted as games (with incomplete information) between various nodes in a network or between a server and a potential malicious attacker. As such, security design is akin to an economics mechanism design problem, and thus standard game theory tools can be used to design security approaches with certain features and/or obtain appropriate risk assessment measures.

Later work will expand on this in several ways. The overall goal of this is to tie compensating controls to elements of the ontology, so developers and users of systems that must secure online financial transactions can determine which controls they should use to ensure any attacks that the systems or their implementations fail to block will prove ineffective or, at worst, will be limited. This is needed since existing, recommended, and/or required controls such as PCI DSS may not be implemented for a variety of technical, legal, economic, and business reasons. The goal of a compensating control is to mitigate this by minimizing an increase in overall risk when an existing, recommended, and/or required control may not be implemented.

First, we expanded and refined the ontology to cover more details of these systems, in particular the details of session management. This is important because attackers focus on details of security systems such as specific controls and their implementations to compromise systems. The ontology will need to include details of both transactions and sessions as well as the compensating controls themselves. In effect, these are two parallel ontologies merged by common points as well as by the relationships between the compensating controls and the ontological components of transactions and sessions.

Next, from this work, we have observed several patterns that we will formalize and develop in subsequent work from both a computer science and a game theory perspective. For example, the pattern we have already developed looked at purchasing products or services from a web merchant. Since this more often than not involves the use of credit card transactions, we employed PCI DSS to represent real-life existing controls. This was done to validate the approach being used by our team. Since the development of design patterns for compensating controls has not been done in this space before, it was important to work with something that is known so a design pattern derived from it could be validated by domain experts. The resulting framework created for this design pattern could then be tested with this known entity — the PCI DSS controls.

To facilitate the development of a larger catalog of design patterns and corresponding compensating controls, we wil be formalizing the ontologies in a description language. Part of this work will be to assess the most appropriate description language for the task given the nature of the domain of the ontology. We will also consider the existing tools that exist for different languages, such as RDF and OWL, that will enable us to visualize our design patterns and perform inference on them. Doing so will support efforts such as design pattern recommendation systems based on the goals of the session design.

After we have decided on the most appropriate technology to formalize our catalog, we will convert our existing ontologies into the formalized language. This step provides a low-cost checkpoint to ensure that the language and tools we have chosen are compatible with our underlying goals. If any issues arise, we will re-examine our design and ensure that we are able to move forward before investing additional resources into a particular technology tool chain. We will also validate the new representation of the ontology by ensuring that it captures the existing security approaches used in our initial design pattern and subsequent design patterns that will be developed.

Once we have a significant formalized catalog, we will move into developing a guidance system for organizations to use. Our goal is to provide a system that is sound and usable by system designers. By sound, we mean that the system will provide the designer with correct advice about compensating controls to reduce risk by taking into account both the benefits and the costs of such measures. By usable, we mean that the system will undergo human-oriented design so that users will choose to use it because it makes their job

easier. We expect that an organization will have goals for what and how their particular system needs to be secured and they will have constraints on how that technology must be used. These will be the inputs to the system and we will provide recommendations of design patterns that will help designers build secure systems. We intend to utilize reasoning tools that process our ontologies to ensure that the system is as automated and extensible as possible.

A. Limitations

For purposes of this project, we adopt the definition of a design pattern as something that describes a recurring problem that occurs in a particular situation and under a set of requirements and recommends a solution to this problem [7]. Of course, the variables of such problems and requirements in the real world that can affect IdM systems are myriad, and many legal and economic variables dont lend themselves to easy measurement of the sort that might be usefully applied in developing technical systems.

Nonetheless, these socio-technical system variables can yield to analysis and measurement, as is demonstrated by massive activity in metric-driven markets, commerce, and finance and the national, local and private infrastructures of laws, regulations and contracts. Each of these domains of technical, economic and legal engagement has generated its own set of performance variables relevant to their respective stakeholders. Unsurprisingly, design patterns also appear in each of these domains. Our project is intended to make the design goals and metrics of each domain more accessible to the other domains to aid in the better integration of security for IdM in real world sessions and transactional and behavioral contexts.

Given the many potential variables, we limit this work initially to harvesting design patterns for compensating controls from the relatively mature IdM systems used in the banking and financial sectors. This will provide us with a stable base from which to expand their application into the distributed and extended supply chains and economic and legal variables that affect IdM in other real world settings. We limit the scope of the design patterns for compensating controls that we include in this project to those patterns, and IdM related security problems, that arise in session management.

Patterns arise at different levels of abstraction. Our focus is on the higher-level architectural patterns that can be helpfully cross-referenced by developers seeking interoperability and scalable performance for their IdM solutions.

These architectural design patterns are more platform independent than implementation patterns, which demonstrate implementation for a particular technology. Our work focuses on cataloging and framing architectural design patterns, recognizing that implementation patterns are often more proprietary, platform specific, and of more constrained interoperability. Nonetheless, these architectural design patterns lend themselves to the implementation of compensating controls across technological systems.

Another limitation to adoption is the possible perception by organizations that their customized implementation patterns and compensating controls at the implementation level are in some way “proprietary” or that they offer a valuable competitive differentiation or advantage because of their uniqueness. To the extent that this is the case, that organizational perception might be overcome by evidence that the adoption of the design patterns for compensating controls produced in this project offers superior risk mitigation to that of those existing customized, in-house solutions. This shift is made possible by the fact that organizations increasingly share information infrastructures where unilateral security solutions frequently are rendered inferior by group action such as adopting best practices or standards.

B. Audience

This project seeks to help IdM system designers, operators, users and auditors to make better informed decisions about the security, integrity and predictability of identity systems at all stages of the IdM product and service lifecycle. There are many decisions that go into the design, development, deployment, operation and use of a given identity system, all of which depend on the requirements of the particular solution. This project produced materials and resources for developers, and other parties in the IdM “supply chain” to help them to more quickly and easily make appropriate IdM-related decisions in a given context. Future work will expand beyond the initial design pattern and compensating controls developed.

As was the case with earlier security design patterns initiatives such as in the Web Services Area, those parties involved in designing, developing and deploying security and identity systems in sessions and transactional management contexts will gain the greatest benefit from the deliverables of this project.

This project has the potential to result in IdM systems for managing sessions and transactional (behavioral) risks becoming less costly, more scalable, more interoperable, more amenable to standardization, more auditable, more transparent and open and more broadly trustworthy.

People and institutions already benefit from existing design patterns processes and from applying compensating controls in their security approaches that were both developed prior to this project. Our intention is to extend the benefit of design patterns for compensating controls to a broader range of systems, with initial focus of this project on IdM systems of banking and financial entities bringing benefits of these disorder-resisting processes and architectures to a broader population of users.

IV. Implementation

The goal of this project is to present procedural and technical design patterns to provide the desired level of security.

For purposes of this description, a *session* is a communication between endpoints that carries out a transaction. A *transaction* is any activity related to a single goal. For example, withdrawing money from an ATM is a transaction between

a customer and a bank. But this transaction is composed of other transactions.

1) The customer carries out a transaction with the ATM to request and obtain her money.
2) The ATM carries out a transaction with the banks computers to request and obtain authorization to satisfy the request.

Each of these transactions constitutes a session; those sessions are sub-sessions of the main session. They too can be further decomposed into a series of human-computer sessions between the customer and the ATM, and network sessions between the ATM and the bank computer.

Each of these sessions has a set of properties that must be satisfied. For example, the property of accurate identification is present in the ATM to bank computer session (and vice versa). It is present in the human to ATM session, but not in the ATM to human portion; that is why ATM skimmers work.

The next goal is to characterize the attributes of a session relevant to the goals of the transaction. Our hypothesis is that the attributes can apply at any level of session. Which ones to apply depend solely on the goals of the underlying transaction.

A. Objective

We are trying to improve the reliability and resilience of IdM sessions by applying design patterns, and extending these design patterns to include compensating controls.

B. Novelty

While work has been previously undertaken by others to enhance the interoperability of extended chains of technology in certain aspects of IdM (such as in the case of "federated identity" systems), we are not aware of the application of design patterns processes to discern patterns of multiple-technologies supplied by multiple providers working in tandem in the real world. Also, we are not aware of any prior work on applying design patterns for compensating controls to hybrid systems of technology, economics and legal variables working in critical infrastructure supply chains.

Many of the threats and vulnerabilities of IdM systems arise as the result of business and economic factors that have not historically been taken into account in earlier design patterns efforts. The result is that these factors remain unaddressed in current system design and development work, leading to significant additional costs for system operators and users. If the integration of hybrid business, legal, and technical (BLT) design patterns can help to mitigate these persistent threats and vulnerabilities, it will release value for the stakeholders in these systems, offering potential additional resources for further development of the work beyond our initial project. De-risking has value for the benefited parties.

C. Technical Challenges

The technical challenges inherent in our solution include the costs of altering technology (hardware and software) systems relied upon in banking, which tend to be capital intensive and to be deeply integrated into the other systems (such as payments, CRM, contract management, etc.) of this highly regulated domain. This is the "legacy systems" problem. It may also require changes in procedures due to changes in technology, which incurs additional cost. Of course, our focus is on the IdM elements of those systems, which generally reflect a more modest portion of such capital costs and can sometimes have stand-alone functionality enabling their substitution.

D. Potential for Success

Our solution is based on the concepts of design patterns for compensating controls that have already demonstrated their value in technical system design, development, and deployment in the real world. That provides a solid foundation for the expansion of these concepts into more extended technical supply chains and hybrid supply chains associated with sessions and transactional management.

Our initial design pattern and compensating controls and ones that will be developed in future work will help organizations save money, increase leverage, and reduce threats. Once these qualities are demonstrated to commercial and governmental organizations, both of which are obliged to limit costs, they will be economically compelled to implement these processes and architectures. It is not easy to predict the precise timing of how quickly such advances will be adopted, but it is clear that commercial enterprises and governments (with budget pressures) cannot afford to leave extra value on the table.

Our confidence in the project is based on the fact that the processes that we will apply have demonstrated their value in other, narrower contexts. We also think that organizations with responsibilities for banking/financial services have been frustrated by the limited options available to make their systems cyber secure, and are ready to entertain new approaches to securing the IdM elements. The design patterns and associated compensating controls being developed herein represent a low risk and high reward calculus for organizations and thus we believe will result in high utilization by various stakeholders.

E. Looking Ahead

Ultimately, the success of the project will depend on whether it contributes to de-risking sessions management and transactional/behavioral management elements of IdM. Because it is difficult to measure negative effects, the ultimate measure of attacks and accidents prevented can be difficult despite the number of attacks targeting financial systems [8]. However, given the demonstrated value of both design patterns in propagating good practices in software design and development, and of compensating controls in providing functional compromises, we are anticipating that the cost/benefits analysis of implementing our projects prototypes and frameworks for identity management will encourage adoption and implementation.

References

[1] Abdulrahman Alarifi, Mansour Alsaleh, and Noura Alomar. A model for evaluating the security and usability of e-banking platforms. *Computing*, 99(5):519535, 2017.

[2] David J Bederman. *Custom as a Source of Law*. Cambridge University Press, 2010.

[3] Jan O. Borchers. A Pattern Approach to Interaction Design. In *Proceedings of the 3rd Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques*, DIS '00, pages 369–378, New York, NY, USA, 2000. ACM. event-place: New York City, New York, USA.

[4] Marc Dupuis and Samreen Khadeer. Curiosity killed the organization: A psychological comparison between malicious and non-malicious insiders and the insider threat. In *Proceedings of the 5th Annual Conference on Research in Information Technology*, pages 35–40. ACM Press, 2016.

[5] Aldo Gangemi. Ontology Design Patterns for Semantic Web Content. In Yolanda Gil, Enrico Motta, V. Richard Benjamins, and Mark A. Musen, editors, *The Semantic Web ISWC 2005*, Lecture Notes in Computer Science, pages 262–276. Springer Berlin Heidelberg, 2005.

[6] Matthew Hoekstra, Reshma Lal, Pradeep Pappachan, Vinay Phegade, and Juan Del Cuvillo. Using innovative instructions to create trustworthy software solutions. *HASP@ ISCA*, 11, 2013.

[7] Jason Hogg, Don Smith, Fred Chong, Dwayne Taylor, Lonnie Wall, and Paul Slater. *Web service security: Scenarios, patterns, and implementation guidance for Web Services Enhancements (WSE) 3.0*. Microsoft Press, 2005.

[8] Navjeet Kaur. A survey on online banking system attacks and its countermeasures. *International Journal of Computer Science and Network Security (IJCSNS)*, 15(3):57, 2015.

[9] C. Kramer and L. Prechelt. Design recovery by automated search for structural design patterns in object-oriented software. In *Proceedings of WCRE '96: 4rd Working Conference on Reverse Engineering*, pages 208–215, November 1996.

[10] Wolfgang Pree. *Design Patterns for Object-oriented Software Development*. ACM Press/Addison-Wesley Publishing Co., New York, NY, USA, 1995.

[11] Dirk Riehle and Heinz Zllighoven. Understanding and using patterns in software development. *Theory and Practice of Object Systems*, 2(1):3–13, 1996.

V. Appendix

Note: Some sample text from the design pattern and compensating controls that were developed is included in the template that follows for context. To see the full design pattern and compensating controls that were developed, please visit: http://www.aristotle.cc/Pattern$_1$.pdf

Design Patterns for Compensating Controls Template

Problem

A customer C wants to complete a purchase from merchant M using a credit card over the web.

Intent

Provide a secure mechanism for a customer to complete a purchase from a merchant via an online financial transaction over an inherently insecure Internet.

Applicability

Consider a customer C purchasing something from a merchant M on the World Wide Web. C uses a credit card. This goes to a transaction clearing center S that approves or disapproves the transaction.

Requirements

1. The order and payment information is transmitted among C, M, and S in such a way that the transaction is visible only to those three parties, and it cannot be altered without the consent of both C and M

2. C, M, and S are authenticated to one another as being a party to the transaction

...

Entities

1. C, customer (or authorized delegate of the customer) making an order and paying for it

2. M, the merchant who will process the transaction

3. S, the transaction clearing center

Requirements for Entities

1. All must both be able to do hashing and both public key and symmetric cryptography

2. All must have sufficient connectivity so they can exchange messages reliably

...

Solution

1. C puts order and payment information into a message m (in encrypted form if required by law).

2. C sends m to M using a secure channel (in encrypted form if required by law).

...

Consequences

1. C is assured it is ordering from M

2. M is assured the order and payment information comes from C

...

Assumptions

1. Secure means all parties were properly identified, authenticated and authorized, integrity checked, and confidential.

2. A purchase is either allowed or disallowed by S. No conditions to either can be attached. [truncated]

Implementation

[omitted here; see online document]

Attacker Models

[omitted here; see online document]

Definitions

[omitted here; see online document]

Control #3: Direct Internet Access Prohibited

Control #3 Name	Prohibit direct access between the Internet and any system component in the transaction (PCI DSS (legal) requirement 1.3)
Type of Control	☒ Technical ☐ Business/Economic ☒ Legal
Description	All transactions to and from S must go through the firewalls
Reason #1 for Non-Implementation of Existing Security Control	
Rationale	The network is complex and it is difficult to assure that no connections go through any other network egress point. For example, a system may be connected to a modem/telephone line for ease of remote administration.
Type of Reason	☒ Technical ☒ Business/Economic ☐ Legal
Impact	Unauthorized personnel may obtain access through this secondary channel
Impact Area(s)	☒ Confidentiality ☒ Integrity ☒ Availability ☐ Business ☐ Legal
Impact Description	If the transaction server allows remote connections for administration, and those connections may originate external to the network, then an attacker could attempt to access this capability and modify the transaction server through malicious administration. The attacker could also read credit card numbers and other information in this case. Or, they could simply flood the transaction server, making it unavailable.
Compensating Control(s) for Reason #1	
Compensating Control #1	Disconnect all modems and block all ports (USB and others) that could be used to connect to a network that does not go through the firewall. Note the disallowed network need not be the Internet; but it must be connected (or able to connect to) to the Internet.
Type of Compensating Control	☒ Technical ☐ Business/Economic ☐ Legal
Description	Any network communication to the Internet must go through the single network connected to the server, and hence through the firewall.
Reason #2 for Non-Implementation of Existing Security Control	
Rationale	See Reason #2 and CC #2 for Control #2
Type of Reason	☐ Technical ☒ Business/Economic ☒ Legal
Impact	See Reason #2 and CC #2 for Control #2
Impact Area(s)	☐ Confidentiality ☐ Integrity ☐ Availability ☐ Business ☐ Legal
Impact Description	See Reason #2 and CC#2 for Control #2
Compensating Control(s) for Reason #2	
Compensating Control #1	See Reason #2 and CC#2 for Control #2
Type of Compensating Control	☐ Technical ☐ Business/Economic ☐ Legal
Description	See Reason #2 and CC#2 for Control #2

Fig. 1. Example of a control, reasons why it may not be fully followed, and recommended compensating controls