UTAH INLAND PORT AUTHORITY

Internal Control Program

Document Number:	BP-09	**Version:**	2.1
Initial Effective Date:	December 2019	**Last Revision Date:**	
Policy Owner:	Amy Brown Coffin	**Approved By:**	Amy Brown Coffin

Table of Contents

Revision Table

Version	Effective Date	Revision Author	Summary of Revisions
2.1		Amy Brown Coffin	Changed from PO-10 to BP-09; Update title from Director of Compliance to Chief Compliance Officer in Roles & Responsibilities
2.0	January 20, 2022	Amy Brown Coffin	Added Definitions and Roles & Responsibilities Tables; Enhanced and defined processes for risk assessment, internal controls, control testing, and corrective actions

I. Purpose Statement

This policy was developed to assist the Utah Inland Port Authority (UIPA) in the implementation, assessment, and maintenance of good internal controls over agency operations, financial reporting, and compliance.

II. Regulatory / Legislative Requirements

None

III. Scope

This policy covers the risk and internal control framework and process for the UIPA compliance program for all UIPA employees, contractors, interns, partner, and vendors.

IV. References

- FIACCT 20-00 Internal Controls
- COSO Internal Control Integrated Framework

V. Definitions

Term	Definition
Control Test	A periodic validation that ensures the control is working effectively.
Corrective Action	Step-by-step plan designed and implemented to address and correct those issues or deficiencies, as well as facilitate ongoing compliance activities.
Inherent Risk	The amount of risk that exists in the absence of controls.
Internal Control	A process designed to provide reasonable assurance that agency objectives are achieving effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations.
Pillar or Process	A risk category of connected organizational processes or areas.
Residual Risk	The amount of risk that remains after controls are accounted for.
Risk	The threat posed to a company's financial, organizational, or reputational standing resulting from violations of laws, regulations, codes of conduct, or organizational standards of practice.
Risk Impact	The impact of a risk event to the organization and its ability to achieve desired results and objectives.
Risk Probability	The likelihood of a risk event occurring.
Risk Severity Score	Average risk impact score + average risk probability score

VI. Roles & Responsibilities

Role	Responsibility
Chief Compliance Officer	Oversee Compliance program and strategy including risk identification and assessment, internal control creation and implementation, control testing, and correction action documentation and remediation.
Pillar / Process Owner	• Helps identify and associate existing risks to process / pillar • May propose risk owner • Approves description and assignment of related policies, procedures, and records • Determines inherent risk • Assesses associated risk probability and impact
Control Owner	• Recommend control test • Propose control test owner • Approve control description • May assess related risk probability and impact • Regularly review internal control according to predetermined control review frequency
Risk Owner	• Recommend controls to mitigate risk • Propose control owner • Approve risk description, inherent risk, residual risk, person(s) impacted, and source of risk • Assess risk probability and impact • Regularly review risk according to predetermined risk review frequency
Test Owner	• Recommends test frequency • May propose tester • Approves testing steps • May assess related risk's probability and impact
Corrective Action Owner	• Draft and approve root cause, and corrective action plan • Manage the corrective action plan

VII. Policy

This policy is established to reduce risk of fraud and errors in financial statements and reports; risk of loss, misuse, or waste of taxpayer dollars or other assets; risk of noncompliance with state and federal laws, policies, and procedures; and assist the agency in fulfilling their internal responsibilities.

Internal controls consist of five interrelated components: control environment, risk assessment, control activities, information and communication, and monitoring activities. These five components are derived from the way in which management runs operations and how they are integrated throughout the management process. In establishing effective and efficient operations, all five components are required to be present for an internal control program.

VIII. Control Environment

UIPA's control environment begins with the tone at the top. The objective of UIPA's control environment is to ensure that ethics and integrity that includes living the code of conduct, adhering to policies, and embracing organizational values. Effective controls are created through implementing compliance structures and processes with a foundation based upon proper risk management that includes preventative, detective, and responsive controls. Compliance structures ensure that the code of conduct and requirements to abide by the law is effectively implemented. Compliance processes include an analysis of legal risks, publishing and implementing internal regulations, training, and handling concerns and infringements.

The following principles support the control environment:

- The UIPA demonstrates a commitment to integrity and ethical values.
- The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
- Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
- UIPA demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
- The UIPA holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

IX. Risk Assessment

Risk assessment involves a dynamic and iterative process for identifying and assessing risk to the achieve of objectives. This identification and analysis of risks that may get in the way of achieving agency objectives forms the basis of managing risks. The following principles support risk assessment:

- The UIPA specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
- The UIPA identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
- The UIPA considers the potential for fraud in assessing risks to the achievement of objectives.
- The UIPA identifies and assesses changes that could significantly affect the system of internal control.

Risks include but are not limited to environmental & health, external events, financial, information security & operational technology, people, political, project, regulatory & legal, reputational, and vendor risk categories, also referred to as risk processes or pillars. Risks will be assigned to one or more processes / pillars to provide holistic risk oversight. All process / pillars will be assigned a risk owner.

All risks will be assigned a risk owner. Risk owners will ensure that the risks have been appropriately identified, documented, and mitigated through internal controls. Risk documentation will include capturing: risk number, risk title, risk owner, status, risk statement, control

requirements, review frequency, inherent risk, residual risk, person(s) impacted, source of risk, risk probability, risk impact, risk severity score, and key dates.

Risk impact and probability are assessed upon initial risk intake and ongoing review iterations.

Risk Probability Scale

Highly Likely	Risks in the highly likely category are almost certain to occur. Typically, risks with 91 percent or more likelihood fall into this category.
Likely	A likely risk has a 61-90 percent chance of occurring. These risks need regular attention, as they are bound to reoccur and therefore require a consistent mitigation strategy.
Moderate	Moderate risks may happen about half the time — they have a 41-60 percent chance of occurring and need attention.
Unlikely	Risks in the unlikely category have a relatively low chance of occurring — 11 to 40 percent. But they may still affect your business, so it's a good idea to keep an eye on them.
Rare	Rare risks are exactly as they sound, with a less than 10 percent chance of occurring.

Risk Impact Scale

Extreme	A risk event, that if it occurs, will have a severe impact on achieving desired results, to the extent that one of more of UIPA's critical outcome objectives will not be achieved.
Major	A risk event, that if it occurs, will have a significant impact of achieving desired results, to the extent that one of more of UIPA's stated outcome objectives will fall below acceptable levels.
Medium	A risk event, that if it occurs, will have a moderate impact of achieving desired results, to the extent that one of more of UIPA's stated outcome objectives will fall well below goals but above minimum acceptable levels.
Minor	A risk event, that if it occurs, will have a minor impact of achieving desired results, to the extent that one of more of UIPA's stated outcome objectives will fall below goals but well above minimum acceptable levels.
Trivial	A risk event that, if it occurs, will have little or no impact on achieving UIPA's outcome objectives.

Risk severity scores will be calculated based upon key stakeholder, risk owner, pillar / process owner, and executive leadership risk assessment. Risk mitigation efforts and reviews will be prioritized and reassessed based upon risk severity scores as well as association to a regulation, standard, or statute according to the following:

- Biannually: Risk Severity Score > 7 or associated regulation, standard, or statute
- Annually: Risk Severity Score > 4 & < 7
- Biennially: Risk Severity Score < 4

X. Control Activities

Control activities include internal control management through the creation of policies and procedures that help ensure that management's directives to mitigate risks to the achievement of

objectives are carried out. Control activities are performed at all levels of the organization, at various stage within program processes, and over the technology environment.

The following principles support control activities:

- The UIPA selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
- The UIPA selects and develops general control activities over technology to support the achievement of objectives.
- The UIPA deploys control activities through policies that establish what is expected and procedures that put policies into action.

An internal control is associated to at least one or more risks. All internal controls will be assigned a control owner. Control owners will ensure that the internal controls have been appropriately identified, documented, and updated. Internal control documentation will include capturing: control number, control title, control owner, status, control type, control testing requirement, control description, review frequency, and key dates.

Control types are detective or preventative. A detective control is designed to discover an unintended event or result after the initial processing has occurred but before the ultimate objective has concluded (e.g., issuing financial reports). A preventive control is designed to avoid an unintended event or result at the time of initial occurrence (e.g., upon initially recording a financial transaction). Controls that are created due to a corrective action considered responsive and will be classified as detective or preventative.

Internal controls will be created and associated to a risk based upon the following requirements:

- Control Required: Risk Severity Score > 7 or associated regulation, standard, or statute
- Control Recommended: Risk Severity Score > 4 & < 7
- Control Optional: Risk Severity Score < 4

Internal controls will be reviewed based upon their associated risk severity scores as well as association to a regulation, standard, or statute according to the following:

- Biannually: Risk Severity Score > 7 or associated regulation, standard, or statute
- Annually: Risk Severity Score > 4 & < 7
- Biennially: Risk Severity Score < 4

For internal controls with more than one associated risk, the more frequent review period will be designated for the control.

XI. Information and Communication

Capturing information and communicating to the right people in a timely manner enabling individuals to make decisions and carry out their responsibilities. It is also important that the message from the top of the agency is clearly stated that control responsibilities are a top priority.

The following principles support information and communication:

- The UIPA obtains or generates and uses relevant, quality information to support the functioning of internal control.

- The UIPA internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
- The UIPA communicates with external parties regarding matters affecting the functioning of internal control.

Compliance risks, controls, control testing, and corrective actions will be documented and retained in a centralized system of record for efficient reporting.

XII. Monitoring Activities

Internal control systems need to be monitored over time, both through ongoing activities and separate evaluations. Monitoring activities include by are not limited to control testing, corrective actions, internal audit, post-audit reviews, and sustainability testing.

The following principles support monitoring activities:

- The UIPA selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
- The UIPA evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Control Testing

Control testing will be created and associated to an internal control based upon the following conditions:

- Control Test Required for (1) or more associated related controls: Risk Severity Score > 7 or associated regulation, standard, or statute
- Control Test Recommended: Risk Severity Score > 4 & < 7
- Control Test Optional: Risk Severity Score < 4

All control tests will be assigned a control owner. Control test owners will ensure that the control tests have been appropriately documented and updated. Control testing documentation will include capturing: test number, test title, test owner, status, testing steps, and test frequency.

The frequency of which control tests are performed are dependent upon the risk and control mitigation; however, at minimum a control test should be performed annually. All control tests will be assigned a control test owner. The control test owner may also be the individual that performs the control testing.

Additionally, control tests will be reviewed based upon their associated risk severity scores as well as association to a regulation, standard, or statute according to the following:

- Biannually: Risk Severity Score > 7 or associated regulation, standard, or statute
- Annually: Risk Severity Score > 4 & < 7
- Biennially: Risk Severity Score < 4

Corrective Actions

Corrective actions are essential for improving internal controls, enhancing control testing, ensuring compliance, and mitigating risk. Corrective actions may be identified from monitoring activities, audits, testing, or other process gaps or issues.

Any proposed corrective action is to be submitted to the Chief Compliance Officer for review. All corrective actions will be assigned a corrective action owner. Corrective action owners will ensure that the corrective action steps have been appropriately documented and completed. Corrective action documentation will include capturing: corrective action number, corrective action title, corrective action owner, status, priority risk rating, who identified the issue, issue description, root cause, corrective action plan, and key dates.

The targeted due date for the corrective action plan will be dependent upon the risk remediation and impact of the issue. The more significant the impact, the faster the closure date. The dates will be discussed and approved by the corrective action owner and Chief Compliance Officer.

Upon closure of the corrective action plan, the corrective action may be entered into sustainability testing to ensure long term remediation of the corrective action plan.