INTEGRATIONS DEVELOPMENT STANDARDS

**This document is meant to maintain standards across integrations on Workday projects. Following these standards will help with maintenance and posterity across the integrations team and allow for consistent and standardized methodology across projects.**

## APPENDIX

* Naming Conventions
* Security
* Error Handling
* Studio Assemblies
* XSLT Standards
* EIB Standards
* Custom Report Standards

## NAMING CONVENTIONS

## INTEGRATION

INTXXXX [Vendor] [Description] [Direction]

XXXX: integration number (INT0001)

Vendor: The vendor for the integration.

Direction: inbound or outbound with regards to Workday

Description: The general purpose of the integration. This should be very short. (Demographic)

Examples:

INT0001 Merrill Lynch Demographic Outbound

INT0105 Aetna Leave of Absence Inbound

## INTEGRATION REPORTS (FOR EIBS AND STUDIOS)

CRI INTXXXX [Description]

CRI: Custom Report for Integrations

XXXX: Integration number

Description: The purpose of the report

Examples:

CRI INT0025 Dependents and Beneficiaries

CRI INT0105 Leave Types

## Tagging

All reports that are used in integrations should be tagged to “Integrations”!

## INTEGRATION CALCULATED FIELDS

CFI [Description] [Type]

CFI: Calculated Field for Integrations

Description: short description of what the calc field is doing

Type: Calculated Field Type (see below for all abbreviations)

Examples:

CFI Custom ID 1 LRV

CFI Employee ID + Name CON

## INTEGRATION SERVICES AND SEQUENCE GENERATORS

INTXXXX [Type of Services] [Detail]\*

\*Detail is only needed for services that are called out below.

Type of Service

* Field Override – Detail: field override object
* Delivery
* Retrieval
* Sequence Generator
* Integration Map (Mapping)
* Integration Attribute (Attributes)
* Custom Object – Detail: primary object
* Transaction Log

Examples:

INT0001 Field Override – Worker

INT0001 Sequence Generator

## INTEGRATION SECURITY USERS

ISU INTXXXX [Integration Name]

XXXX: Integration Number

Integration Name: Copy the integration name for which the ISU is being used.

Example:

ISU INT0001 CCW Outbound File Name

## INTEGRATION SECURITY GROUPS

ISSG INTXXXX [Integration Name]

XXXX: Integration Number

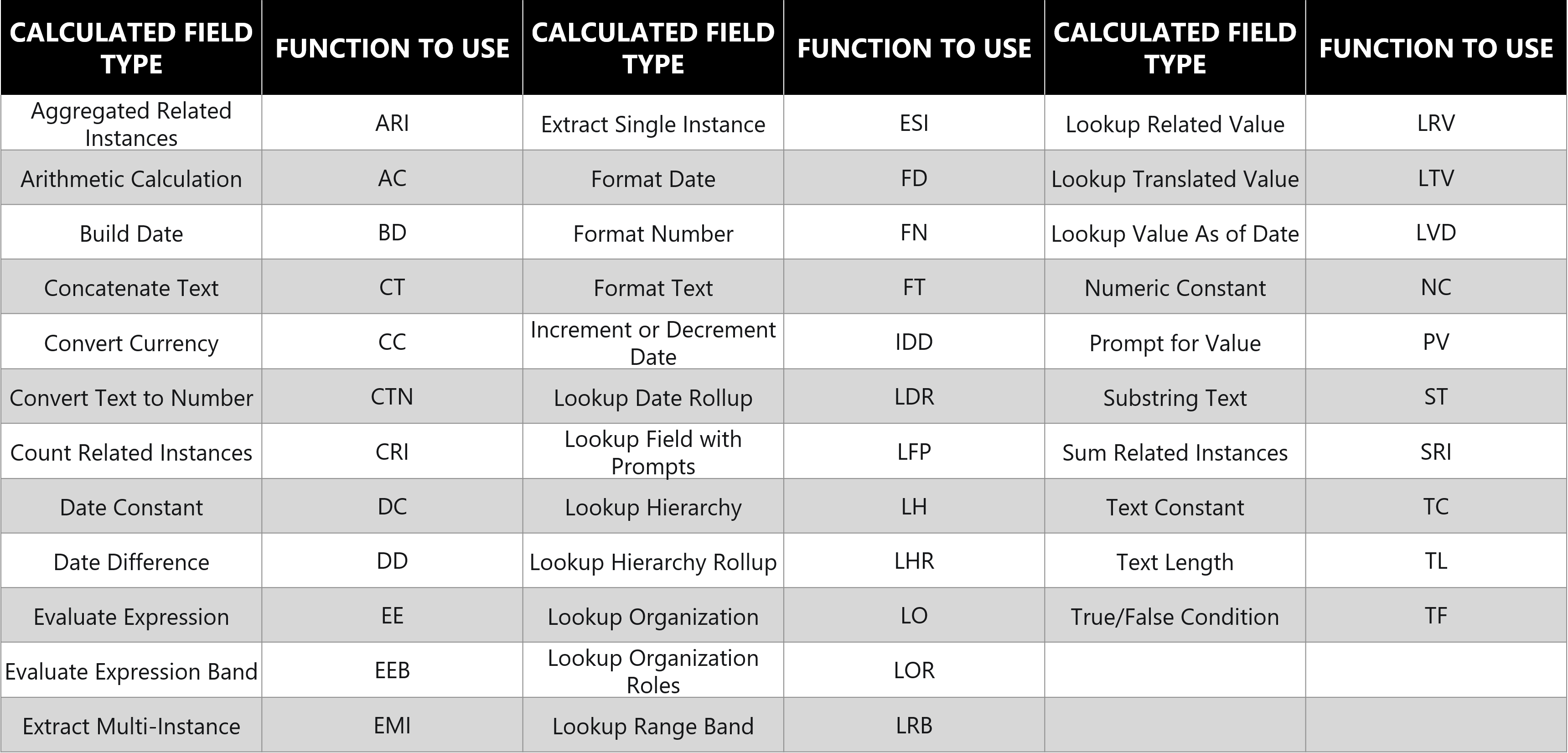
Integration Name: Copy the integration name for which the ISSG is being used.

Example:

ISSG INT0001 CCW Outbound File Name

NOTE: Workday defaults your ISSG Reference ID to “Integration\_Security\_Group\_12345”. You MUST edit the Reference ID for each ISSG that you create to have a human-readable ID. Simply change the spaces in your ISSG name to underscores for your Ref ID. (i.e. if your ISSG name is ISSG INT123 Worker Data Outbound, the ref ID should be ISSG\_INT123\_Worker\_Data\_Outbound).

## CACULATED FIELD ABBREVIATIONS



## Key Naming Conventions

[Type of key] [Vendor] [Tenant]

Type of key: This can either be x509 or PGP, depending on if the key is being used for authentication or for encryption.

Tenant: This is being included because the first keys that are sent in the Configure & Prototype phase will need to be changed when we enter the End-to-End phase. After go-live, there will need to be a key for Production and one for Sandbox, and this also reduces the confusion for these scenarios. Examples: C&P, E2E, PARALLEL, PROD, SBX

## SECURITY

Following Workday’s prescribed best practices, the standards for integration security users and security groups are below:

* There must be one Integration Security User (ISU) for each Integration System Security Group (ISSG), and vice-versa. This is so that we can build a prescribed security setup for each integration independently, giving it exactly the amount of security necessary to run correctly.
* The ISU will own the integration system, any subsequent integration systems within the same business process, and any reports used within these integration systems.
* The ISU will own integration schedules after go-live.
* The ISU requires a password when it is created. The password should be a random combination of alpha-numeric characters.

## ADDING SECURITY POLICIES TO SECURITY GROUPS

* To correctly add a security policy to an Integration System Security Group, go to the View Domain Security Policy for the specific security policy that you want to add. At the bottom of the page, use the Edit Permissions button and add your security group.
* **If the only option listed at the bottom of the screen is Override Parent Permissions, then DO NOT CLICK THAT BUTTON.** Instead, look for the Parent Policy at the top of the page. Edit Permissions on the Parent Policy and add your security group there instead.

